

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

01 - 15 Jun 2024

Vol. 11 No. 11

Table of Content

Vendor	Product	Page Number
Application		
10web	photo_gallery	1
83pixel	simple_cod_fees_for_woocommerce	3
actpro	extra_product_options_for_woocommerce	3
acurax	under_construction_\/_maintenance_mode	3
Adobe	experience_manager	4
apport_project	apport	152
ARM	bifrost_gpu_kernel_driver	153
THAIN.	valhall_gpu_kernel_driver	154
arwebdesign	dashboard_to-do_list	154
authlib	authlib	155
autowriter	ai_post_generator_\ _autowriter	155
Avast	antivirus	156
awplife	image_gallery	157
awpine	slider_responsive_slideshow	157
bakery_online_ordering_ system_project	bakery_online_ordering_system	158
beyondtrust	beyondinsight	159
Bitdefender	gravityzone	160
born05	two-factor_authentication	160
bosathemes	bosa_elementor_addons_and_templates_for_w oocommerce	161
brizy	brizy-page_builder	162
buddyboss	buddyboss_platform	165
buddypress_cover_proje ct	buddypress_cover	165
Cisco	finesse	166
clashforwindows	clash	171

Vendor	Product	Page Number
cloudfoundry	cf-deployment	172
cloudiounal y	routing_release	172
Clusterlabs	booth	173
codeless	cowidgetselementor	173
codeparrots	easy_forms_for_mailchimp	174
Codepeople	wp_time_slots_booking_form	174
contact_form_builder_pr oject	contact_form_builder	175
creativethemes	blocksy	175
crmeb	crmeb	176
cyberchimps	responsive	177
cyberenimps	responsive_addons	177
cyrusimap	cyrus_imap	178
dextaz_ping_project	dextaz_ping	178
dreryk	gabinet	179
dulldusk	phpfilemanager	179
elearningfreak	insert_or_embed_articulate_content	180
emailgpt	emailgpt	181
emlog	emlog	181
envothemes	envo_extra	182
envoyproxy	envoy	183
estomed	simple_care	197
eurosoft	przychodnia	197
extendthemes	colibri_page_builder	198
fileorganizer	fileorganizer	199
fivestarplugins	five_star_restaurant_menu	200
formwork_project	formwork	201
Fortinet	fortiwebmanager	201
fujielectric	monitouch_v-sft	204
gaizhenbiao	chuanhuchatgpt	204
gamipress	gamipresslink	205
generatepress	generatepress	206
getawesomesupport	awesome_support	207

Vendor	Product	Page Number
getbrave	brave	207
getshortcodes	shortcodes_ultimate	207
Golang	go	208
grafana	oncall	210
homebrew	jan	211
horea_radu	one_page_express_companion	212
icegram	email_subscribers_\&_newsletters	212
idccms	idccms	213
ipages_flipbook_project	ipages_flipbook	214
	aqua	215
	clion	216
	datagrip	220
	dataspell	225
	goland	229
	intellij_idea	234
Jetbrains	mps	238
	phpstorm	241
	pycharm	245
	rider	250
	rubymine	254
	rustrover	259
	webstorm	260
katello_project	katello	264
la-studioweb	element_kit_for_elementor	265
langflow	langflow	265
lifterlms	lifterlms	266
lunary	lunary	267
lylme	lylme_spage	268
master-addons	master_addons	268
melapress	melapress_login_security	270
meowapps	database_cleaner	270
metagauss	eventprime	271

Vendor	Product	Page Number
metagauss	profilegrid	271
mintplexlabs	anythingllm	272
Mongodb	pymongo	273
moveaddons	move_addons_for_elementor	274
multivendorx	multivendorx	274
netgsm	netgsm	275
netty	netty-incubator-codec-ohttp	276
online_discussion_forum _project	online_discussion_forum	276
	configgrpc	278
opentelemetry	confighttp	278
	opentelemetry_collector	279
opmc	woocommerce_dropshipping	280
oretnom23	online_medicine_ordering_system	280
ovic_importer_project	ovic_importer	281
parisneo	lollms_web_ui	281
pdfcrowd	save_as_pdf_plugin	282
pharmacy\/medical_stor e_point_of_sale_system_p roject	pharmacy\/medical_store_point_of_sale_syste m	283
PHP	php	283
Pimcore	pimcore	295
porty	powerbank	295
pq-crystals	kyber	296
projectdiscovery	interactsh	297
purechat	pure_chat	297
qodeinteractive	qi_blocks	298
	openshift_container_platform	298
Redhat	openshift_distributed_tracing	299
	satellite	299
reputeinfosystems	arforms	300
risethemes	rt_easy_builder	300
royal-elementor-addons	royal_elementor_addons	301

Vendor	Product	Page Number
Rubyonrails	rails	302
salesagility	suitecrm	305
sc_filechecker_project	sc_filechecker	316
seacms	seacms	316
securenvoy	multi-factor_authentication_solutions	317
seedprod	rafflepress	317
select-themes	stockholm	318
Select-themes	stockholm_core	319
sendinblue	newsletter_smtp_email_marketing_and_sub scribe	319
sinaextra	sina_extension_for_elementor	320
softlabbd	integrate_google_drive	320
Solitabbu	upload_fields_for_wpforms	321
Solarwinds	serv-u	321
Solal Willus	solarwinds_platform	322
spiffyplugins	spiffy_calendar	323
spinypiugins	wp_flow_plus	323
stock_management_syste m_project	stock_management_system	324
strategery- migrations_project	strategery-migrations	324
stylemixthemes	mega_menu	325
summar	mentor	325
Sysaid	sysaid	326
themehigh	checkout_field_editor_for_woocommerce	326
themeisle	product_addons_\&_fields_for_woocommerce	327
	buddyforms	327
themekraft	buddypress_woocommerce_my_account_integ rationcreate_woocommerce_member_pages	328
themesflat	themesflat_addons_for_elementor	328
themeum	tutor_lms	329
thenewsletterplugin	newsletter	329
thimpress	learnpress	330

Vendor	Product	Page Number
tickera	tickera	331
tnbmobil	cockpit	331
tribe29	checkmk	332
unlimited-elements	unlimited_elements_for_elementor_\(free_wid gets_addons_templates\)	332
upunzipper_project	upunzipper	333
userproplugin	userpro	334
vanyukov	market_exporter	334
Videowhisper	picture_gallery	335
visualcomposer	visual_composer_website_builder	335
viz	nano_id	336
vollstart	event_tickets_with_ticket_scanner	337
wbcomdesigns	custom_font_uploader	338
weavertheme	weaver_xtreme_theme_support	339
web-audimex	audimexee	339
websupporter_filter_cust om_fields_\&_taxonomie s_light_project	websupporter_filter_custom_fields_\&_taxono mies_light	340
westguardsolutions	ws_form	340
willnorris	open_graph	341
wobbie	mollie_forms	342
woostify	boostify_header_footer_builder_for_elementor	342
wow-company	easy_digital_downloads	343
wow-company	woocommercerecent_purchases	344
wpattire	attire_blocks	344
wpdeveloper	embedpress	345
wpuevelopei	essential_addons_for_elementor	346
wpdownloadmanager	download_manager	347
wpfactory	products_order_\&_customers_export_for_w oocommerce	348
wpfoxly	adfoxly	348
wpvivid	wpvivid_backup_for_mainwp	349
xootix	login\/signup_popup	349

Vendor	Product	Page Number
yithemes	yith_woocommerce_product_add-ons	350
zorem	advanced_local_pickup_for_woocommerce	350
Hardware		
	2tma310010b0001	351
	2tma310010b0003	352
ABB	2tma310011b0001	352
	2tma310011b0002	353
	2tma310011b0003	354
Mitel	6869i_sip	354
	exynos_1080	356
	exynos_1280	358
	exynos_1330	361
	exynos_1380	364
	exynos_2100	366
	exynos_2200	369
	exynos_2400	371
	exynos_850	372
Comeuna	exynos_9110	375
Samsung	exynos_980	375
	exynos_9820	378
	exynos_9825	380
	exynos_990	382
	exynos_auto_t5123	384
	exynos_modem_5123	385
	exynos_modem_5300	388
	exynos_w920	390
	exynos_w930	391
Tendacn	o3v2	392
uniview	nvr301-04s2-p4	392
YMAI	id.charger_connect	393
vw	id.charger_pro	394
Operating System		

Vendor	Product	Page Number
	2tma310010b0001_firmware	395
	2tma310010b0003_firmware	395
ABB	2tma310011b0001_firmware	396
	2tma310011b0002_firmware	397
	2tma310011b0003_firmware	397
Apple	macos	398
Canonical	ubuntu_linux	402
Debian	debian_linux	406
Fedoraproject	fedora	407
Google	android	409
IBM	i	410
Linux	linux_kernel	412
	windows	415
	windows_10_1507	416
	windows_10_1607	416
	windows_10_1809	417
	windows_10_21h1	417
	windows_11_21h2	417
Microsoft	windows_11_22h2	417
Microsoft	windows_11_23h2	418
	windows_server_2008	418
	windows_server_2012	418
	windows_server_2016	419
	windows_server_2019	419
	windows_server_2022	419
	windows_server_2022_23h2	419
Mitel	6869i_sip_firmware	420
	enterprise_linux	422
	enterprise_linux_eus	423
Redhat	enterprise_linux_for_arm_64	424
	enterprise_linux_for_ibm_z_systems	425
	enterprise_linux_for_ibm_z_systems_eus	426

Vendor	Product	Page Number
	enterprise_linux_for_power_little_endian_eus	427
Redhat	enterprise_linux_server_update_services_for_s ap_solutions	428
	exynos_1080_firmware	429
	exynos_1280_firmware	431
	exynos_1330_firmware	434
	exynos_1380_firmware	437
	exynos_2100_firmware	439
	exynos_2200_firmware	442
	exynos_2400_firmware	444
	exynos_850_firmware	445
Samsung	exynos_9110_firmware	448
Samsung	exynos_980_firmware	448
	exynos_9820_firmware	451
	exynos_9825_firmware	453
	exynos_990_firmware	455
	exynos_auto_t5123_firmware	457
	exynos_modem_5123_firmware	458
	exynos_modem_5300_firmware	461
	exynos_w920_firmware	463
	exynos_w930_firmware	464
Tendacn	o3v2_firmware	465
uniview	nvr301-04s2-p4_firmware	465
VAN	id.charger_connect_firmware	466
vw	id.charger_pro_firmware	469

Common Vulnerabilities and Exposures (CVE) Report						
Weakness	Publish Date	ate CVSSv3 Description & CVE ID Patch		Patch	NCIIPC ID	
			Application			
Vendor: 10	web					
Product: ph	oto_gallery					
Affected Ver	rsion(s): * Up to	(excludin	g) 1.8.24			
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Jun-2024	8.8	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.8.23 via the esc_dir function. This makes it possible for authenticated attackers to cut and paste (copy) the contents of arbitrary files on the server, which can contain sensitive information, and to cut (delete) arbitrary directories, including the root WordPress directory. By default this can be exploited by administrators only. In the premium version of the plugin, administrators can give gallery edit permissions to lower level users,	https://plugins. trac.wordpress. org/changeset/ 3098798/	A-10W-PHOT- 200624/1	

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which might make this exploitable by users as low as contributors. CVE ID: CVE-2024-5481		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'svg' parameter in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this can only be exploited by administrators, but the ability to use and configure Photo Gallery can be extended to contributors on pro versions of the plugin. CVE ID: CVE-2024-5426	https://plugins. trac.wordpress. org/changeset/ 3098798/	A-10W-PHOT-200624/2

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description 8	k CVE ID		Patch		NCIIPC ID
Vendor: 83 ₁	oixel		l.					
Product: sin	nple_cod_fees_	for_wood	ommerce					
Affected Ver	sion(s): * Up to	(including	g) 2.0.2					
Missing Authorizati on	09-Jun-2024	8.8	Missing Authorization vulnerability Andreas Some Somple COI for WooComme s issue Simple COI for WooCom from n/a to 2.0.2.	in ofantzis Fees rce.Thi affects Fees merce:	N/A			-83P-SIMP- 00624/3
			CVE ID: 2024-3566	CVE-				
Vendor: act	pro							
Product: ex	tra_product_op	tions_fo	r_woocomme	erce				
Affected Ver	sion(s): * Up to	(excludin	g) 3.0.7					
Missing Authorizati on	10-Jun-2024	8.8	WooComme s issue affect Product Opt WooComme from n/a t 3.0.6. CVE ID:	athorization Ilnerability in Itpro Extra Ioduct Options for IooCommerce.Thi Issue affects Extra Ioduct Options for IooCommerce: Iom n/a through IooCommerce: Iom n/a through IooCommerce: IooCommerce: Ioom n/a through IooCommerce: Ioom n/a through IooCommerce: Ioom n/a through IooCommerce: IooCommerce: Ioom n/a through IooCommerce: IooCommerce		N/A		-ACT-EXTR- 00624/4
Vanda			2024-3572	7				
Vendor: acu		lon \ /	aintana	a a d a				
	der_constructi sion(s): * Up to			noue				
Allected ver	Sion(s): Op to	(menuali)		on				
Authentica tion Bypass	10-Jun-2024	5.3	Authentication Bypass by Spoofing vulnerability in A-ACU-U 200624/			-ACU-UNDE- 00624/5		
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
by Spoofing			Acurax Under Construction / Maintenance Mode from Acurax allows Authentication Bypass.This issue affects Under Construction / Maintenance Mode from Acurax: from n/a through 2.6. CVE ID: CVE-2024-35749		
Vendor: Add	obe				
Product: ex	perience_mana	ager			
Affected Vers	sion(s): * Up to	(excludin	g) 2024.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	6.1	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE-2024-36216		A-ADO-EXPE- 200624/6
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS)	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/7
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	D	escription	& CVE ID		Patch		NCIIP	CID
('Cross-site Scripting')			co am ma in fo Ma Jar ex vid wl to co vu	uld be a attacked alicious to vialicious vascript ecuted ctim's then they	field.	4-28	ager/ap I.html	osb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Market Score of the state of th	anager 5.20 and e affect ored C ripting linerabili uld be a attacker alicious to vi rm alicious vaScript ecuted ctim's hen they	bused by r to inject scripts ulnerable fields. may be in a browser r browse page the field. CVE-	http: dobe ity/perio man 4-28	s://help e.com/so oroducts ence- ager/ap s.html	ecur s/ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page	13-Jun-2024	5.4	M: 6.! ar	anager 5.20 and e affect	xperience versions d earlier ed by a Cross-Site	dobe ity/p	s://help e.com/so products ence-	ecur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CVSSv3 Scoring Scale* stands for all versions

Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26036	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') 13-Jun-2024 5.4 Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-	('Cross-site			vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	4-28.html	
	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	

CVSSv3 Scoring Scale* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE- 2024-26039	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/11
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/12

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-2024-26053		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields Malicious JavaScript may be executed in a victim's browser when they browser when they browser to the page containing the vulnerable field. CVE ID: CVE- 2024-26054	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/13
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/14

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. CVE ID: CVE-2024-26055		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script. CVE ID: CVE-2024-26057	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/15

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. CVE ID: CVE-2024-26058	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/16
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/17

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-2024-26060		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26066	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/18
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/19
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Improper Neutralizat ion of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") Improper Neutralization of Input During Web Page ("Cross-site Scripting") Improper Neutralization of Input During Web Page ("Cross-site Scripting") Improper Neutralization of Input During Very Neutralization of Inpu	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of linput During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of linput During Web Page Corporation ('Cross-site Scripting') Improper Neutralizat ion of linput During Web Page Corporation ('Cross-site Scripting') Improper Neutralizat ion of linput During Improper Neutralizat ion of linput During Neutralizat ion of linput Neutralizat ion vulnerable ion dividualizat ivy/products/ex perience manager/apsb2 A-AADO-EX				containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') 13-Jun-2024 5.4 Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	dobe.com/secur ity/products/ex perience- manager/apsb2	
victini 5 bi owser	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	dobe.com/secur ity/products/ex perience- manager/apsb2	

^{*} stands for all versions

			when they browse to the page containing the vulnerable field.		
			CVE ID: CVE- 2024-26071		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. CVE ID: CVE-2024-26072	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/22
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/23

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26074		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/24
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/25

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26077		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26078	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/26
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/27

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26081		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/28
			2024-26082 Adobe Experience	hu / /hh	
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/29
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26083		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26085	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/30
Improper Neutralizat ion of Input During Web Page Generation CVSSv3 Scoring	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) -3 3-4 4-5	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/31

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CV	E ID	Patch		NCIIP	C ID
('Cross-site Scripting')			referencing vulnerable po- malicious JavaScript con- may be execu- within the con- of the victi- browser.	e to 4-2 m to JRL a age, tent ated text	nager/aps 8.html	b2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	vulnerability could be abused an attacker to in malicious script or field Malicious JavaScript may executed in victim's brown when they brown to the production containing vulnerable field.	ons clier y a Site (SSS) chat l by ject http dokable ity/clds. per mains be 4-2 a vser wse age the	os://helpx be.com/sec products/ ience- nager/aps 8.html	cur 'ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experie Manager versi 6.5.20 and ear Answer: affected by a Do based Cross-	nce httpons dok-lier ity/per DM-	os://helpx be.com/sec products/ ience- nager/aps 8.html	cur 'ex	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. CVE ID: CVE- 2024-26090	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/34

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. CVE ID: CVE- 2024-26091	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/35
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/36

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26093	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/37
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/38

^{*} stands for all versions

			containing vulnerable field.	ge he TE-	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	containing vulnerable field.	ns der	A-ADO-EXPE- 200624/39
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experient Manager version 6.5.20 and early are affected by reflected Cross-Stripting (XX vulnerability. If attacker is able convince a viction visit a Unreferencing vulnerable parallicious JavaScript contents and be executed to the second stription of the second s	https://helpx.a dobe.com/security/products/experience-manager/apsb2 4-28.html	A-ADO-EXPE- 200624/40

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the context of the victim's browser. CVE ID: CVE-2024-26111		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26113	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/41
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/42

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 victim's browser. CVE ID: CVE-2024-26114		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26115	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/43
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/44

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE- 2024-26116			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26117	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/45	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/46	

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE- 2024-26121			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26123	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/47	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/48	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			containing the vulnerable field. CVE ID: CVE-			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-34120	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/49	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/50	

CVSSv3 Scoring Scale
* stands for all versions

Improper Neutralizat ion of Input During Web Page 13-Jun-2			when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36141		
Neutralizat ion of Input During				1	
Generation ('Cross-site Scripting')	2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36142	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/51
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/52

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36143		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36144	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/53
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/54

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36147	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/55
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/56

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description	n & CVE ID	Pat	tch	NCIIP	C ID
			JavaScript executed victim's when the to the containing vulnerable CVE ID: 2024-361	in a browser y browse page the e field.				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Scripting vulnerabil could be a an attacke malicious	versions d earlier ded by a Cross-Site (XSS) ity that abused by r to inject scripts ulnerable fields. may be in a browser y browse page g the e field. CVE-	https://l dobe.com ity/prod perience manager 4-28.htm	m/secur lucts/ex e- r/apsb2	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Scripting vulnerabil could be a an attacke malicious	versions d earlier ted by a Cross-Site (XSS) ity that abused by	https://l dobe.com ity/prod perience manager 4-28.htm	m/secur lucts/ex e- r/apsb2	A-ADO-E 200624/	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36150		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. CVE ID: CVE-2024-36151	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/59
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/60

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36152		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36153	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/61
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/62

^{*} stands for all versions

('Cross-site				D Patch	
Scripting')			an attacker to inject malicious script into vulnerable form field Malicious JavaScript may lexecuted in victim's brows when they brows to the page containing the vulnerable field. CVE ID: CVE 2024-36154	ts de s. de de de ce de	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experient Manager version 6.5.20 and earliare affected by stored Cross-Siscripting (XS) vulnerability the could be abused be an attacker to inject malicious scripting into vulnerable form field Malicious JavaScript may be executed in victim's brows when they brows to the page containing the vulnerable field.	https://helps.cs. https://helps.cs. https://helps.cs. perience-manager/aps.ce 4-28.html	cur /ex A-ADO-EXPE- 200624/63
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experient Manager version 6.5.20 and earliare affected by stored Cross-Siscripting (XS) vulnerability the	dobe.com/se ity/products, perience- manager/aps 4-28.html	cur /ex A-ADO-EXPE- 200624/64

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36156		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36157	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/65
Improper Neutralizat ion of Input During Web Page Generation CVSSv3 Scoring	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) -3 3-4 4-5	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/66

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	De	escription	& CVE ID		Patch		NCIIP	C ID
('Cross-site Scripting')			co an ma int for Ma Jav ex vid wl to co vu	uld be a attacker alicious to virm alicious vaScript ecuted ctim's nen they the ntaining lnerable VE ID:	field.	4-28	ager/ap 3.html	osb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Ac Ma 6.! ar stee Sc vu co am ma int for Ma Jav vice wl to co vu	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious			s://help e.com/so products ence- ager/ap 8.html	ecur s/ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page	13-Jun-2024	5.4	Ma 6.5 ar	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site			s://help e.com/so oroducts ence-	ecur	A-ADO-EXPE- 200624/68	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	B D	escription	& CVE ID		Patch		NCIIP	C ID
Generation ('Cross-site Scripting')			vi cc an m in fo M Ja ex vi w to cc vi	rm alicious vaScript cecuted ctim's hen they	to inject scripts almerable fields may be in a browser page the field.	4-2	nager/ap 8.html	osb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	M 6. an st So vi co an im fo M Ja ex vi w to co vi C'	cripting alnerabili buld be all a attacker alicious to vu rm alicious vaScript cecuted ctim's hen they	versions d earlier ed by a fross-Site (XSS) ty that bused by to inject scripts ulnerable fields may be in a browser browser the field. CVE	http dob ity/ per ma 4-2	os://help e.com/so products ience- nager/ap 8.html	ecur s/ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During	13-Jun-2024	5.4	M 6.	dobe Ex anager 5.20 and e affecte	versions	dok	os://help e.com/so products ience-	ecur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Do	escription	& CVE ID		Patch			NCIIP	PC ID
Web Page Generation ('Cross-site Scripting')			Sc vu co an main for Ma Jav vic wl to co vu	ripting lnerabilit uld be ab attacker alicious to vu rm alicious vaScript ecuted ctim's nen they the ntaining lnerable:	to inject scripts lnerable fields. may be in a browser browse page the field. CVE-		ager/aps	sb2			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Ma 6.! ar sto Sc vu co an ma in for Ma yie will to co vu CV	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36163			s://helpx e.com/se oroducts ence- ager/aps .html	cur /ex		ADO-E 0624/	
Improper Neutralizat ion of Input	13-Jun-2024	5.4	Ma	Adobe Experience Manager versions 6.5.20 and earlier			https://helpx.a dobe.com/secur ity/products/ex			ADO-E 0624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	2	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	perience- manager/apsb2 4-28.html	
			CVE ID: CVE- 2024-36164		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36165	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/73

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36166	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/74
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/75

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36167		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36168 Adobe Experience		Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/76
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/77

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-2024-36169		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36170	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/78
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/79
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Descriptio	n & CVE ID	Patch	NCIIPC ID
			to the containin vulnerabl	g the e field.		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Manager 6.5.20 ar are affect stored Scripting vulnerabi could be an attacked malicious into form Malicious JavaScript executed victim's	abused by er to inject scripts vulnerable fields. t may be in a browser by browse page g the efield.	https://helpx.a dobe.com/secu ity/products/e perience- manager/apsb 4-28.html	ar A-ADO-EXPE- 200624/80
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Manager 6.5.20 ar are affect stored Scripting vulnerabit could be an attacked malicious into verification form Malicious	lity that abused by er to inject scripts vulnerable fields.	https://helpx.a dobe.com/secu ity/products/e perience- manager/apsb 4-28.html	ar A-ADO-EXPE- 200624/81
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4	4-5	5-6 6-7	7-8 8-9 9-10

CVSSv3 Scoring Scale
* stands for all versions

Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Generation ('Cr	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') S.4 Scripting' 13-Jun-2024 S.4 Scripting' S.5 Scripting Scripting S.5 Scripting S				to the page containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site ('Cross-site) Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts Manager versions 6.5.20 and earlier are affected by a stored Cross-Site butters://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/82
Scripting') Into vulnerable form fields. Malicious JavaScript may be executed in a	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/83

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36175		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36176	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/84
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/85

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36177		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36178	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/86
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/87

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36179		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36180	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/88
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/89

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	3	Description	& CVE ID		Patch		ı	NCIIP	CID
				victim's session. Exploitatio issue requirement interaction typically form of coa victim to maliciously web page interact maliciously modified element wapplication CVE ID: 2024-3618	in the nvincing o visit a verafted or to with a verafted before to with a verafted in the control of the contro						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4		Scripting vulnerabili could be al an attacker malicious	versions l earlier ed by a ross-Site (XSS) ty that bused by to inject scripts alnerable fields. may be in a browser browse page the field. CVE-	dobe ity/p perie man	s://help c.com/se oroducts ence- ager/ap .html	ecur e/ex	A-AI 2006		
Improper Neutralizat ion of Input During	13-Jun-2024	5.4		Adobe Ex Manager 6.5.20 and Answer:	versions	dobe	s://help e.com/se products ence-	ecur	A-AI 2006		
CVSSv3 Scoring	Scale 0-1	1-2	2-		4-5	5-6	6-7	7-8	<u> </u>	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-2024-36183	manager/apsb2 4-28.html	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/92

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			specially crafted form. CVE ID: CVE-2024-36184				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36185	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/93		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/94		
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10		

^{*} stands for all versions

to the page containing the vulnerable field. CVE ID: CVE-2024-36186 Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting') Seripting (XS) vulnerability that could be abused by an attacker to inject malicious graps be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36187 A-ADO-EXPE-2024-36187 Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting') Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 13-Jun-2024 5.4 A-ADO-EXPE-2024-36187 Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field. Malicious JavaScript may be executed in a victim's browser versions of the proper of the properties of the properties of the properties of the vulnerable form fields. Malicious JavaScript may be executed in a victim's browser versions of the properties of the properties of the properties of the properties of the vulnerable field. Versions of the	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During 13-Jun-2024 5.4 5.4 Scripting 13-Jun-2024 13				containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') 13-Jun-2024 5.4 Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	dobe.com/secur ity/products/ex perience- manager/apsb2	
	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	dobe.com/secur ity/products/ex perience- manager/apsb2	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36188		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36189	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/97
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/98

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-2024-36190		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields Malicious JavaScript may be executed in a victim's browser when they browset to the page containing the vulnerable field. CVE ID: CVE-2024-36191	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/99
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/100

^{*} stands for all versions

into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36192 Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36193 Adobe Experience Manager (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject manager application of linguity for the page containing the vulnerable field. CVE ID: CVE-2024-36193 A-ADO-EXPE-2024-36193 Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject into vulnerable field. CVE ID: CVE-2024-36193 A-ADO-EXPE-2024-36193 A-ADO-EXPE	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 13-Jun-2024				form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	dobe.com/secur ity/products/ex perience- manager/apsb2	
	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	dobe.com/secur ity/products/ex perience- manager/apsb2	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36194		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36195	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/103
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/104

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	B D	escription	& CVE ID		Patch		NCIIPC ID		
('Cross-site Scripting')			min for M Ja ex vi wi to co vi C'	rm alicious vaScript ecuted ctim's hen they the ontaining alnerable	scripts linerable fields. may be in a browser browse page the field. CVE-						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	M 6. An af ba So vi vi al ex Ja th vi se Ex is in co to sp lin fo th C' 20	JavaScript code in		http dobe ity/p peri- man 4-28	s://help: e.com/se oroducts ence- ager/aps 8.html	ecur /ex sb2	A-ADO-E 200624/		
Improper Neutralizat ion of Input	13-Jun-2024	5.4	M	Adobe Experience Manager versions 6.5.20 and earlier			s://help: e.com/se oroducts	cur	A-ADO-E 200624/		
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8 8-9	9-10	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	perience- manager/apsb2 4-28.html	
			CVE ID: CVE- 2024-36198		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36199	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/107

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36200	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/108
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/109

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36201		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36202	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/110
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/111

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-2024-36203		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36204	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/112
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/113
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. CVE ID: CVE-2024-36205		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-36206	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/114
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/115

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-2024-36207		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36208	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/116
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/117
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-36210	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/118
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 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	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/119

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 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 victim's browser. CVE ID: CVE-2024-36211		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36212	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/120
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/121
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. CVE ID: CVE-2024-36213		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36214	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/122
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/123

CVSSv3 Scoring Scale
* stands for all versions

Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During (XSS) vulnerability that could be abused by an attacker to inject malcious scripts into vulnerable form fields. Nalicious JavaScript may be	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')				to the page containing the vulnerable field. CVE ID: CVE		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') 13-Jun-2024 5.4 Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	
executed in a	Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields Malicious JavaScript may be	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36218		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36219	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/126
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/127

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. CVE ID: CVE-2024-36220		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36221	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/128
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/129

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/130

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Des	Description & CVE ID				atch		NCIIP	CID
			exec CVE	cute.	script to CVE- 24						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Mar 6.5.2 are stor Scri vulr coul an a mal into form Mal: Java exec victi whe to conf vulr	nager 20 and affecte ed C pting nerabili ld be al ttacker icious sicious cuted im's en they the taining	to inject scripts linerable fields may be in a browser browse page the field.	t ht do ity pe de 4-	be.co y/pro erienc	er/ap	ecur s/ex	ADO-E	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Mar. 6.5.2 are DON Site vulr allo execute yier is sure in the sure in the sure in the sure in the sure is sure in the sure	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user			be.co y/pro erienc	er/ap	ecur s/ex	ADO-E	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6		6-7	7-8	 8-9	9-10

^{*} stands for all versions

			interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-2024-36227 Adobe Experience Manager versions		
			=		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/133
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/134

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-2024-36229		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/135

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36230		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. CVE ID: CVE- 2024-36231	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/136
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36232		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a malicious link. CVE ID: CVE- 2024-36233	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/138
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/139

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-2024-36234		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. CVE ID: CVE- 2024-36235	https://helpx.a dobe.com/secur ity/products/ex perience-manager/apsb2 4-28.html	A-ADO-EXPE-200624/140

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. CVE ID: CVE- 2024-36236	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/141
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/142

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description &	CVE ID	Patch		NCIIP	CID
			click on a mallink or to in with a malic crafted web p CVE ID: 2024-36238	iteract ciously age.				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Scripting vulnerability. vulnerability allow an attace execute ark JavaScript context victim's br session. Exploitation issue require interaction, so convincing a to click of	rsions earlier are DOM-ss-Site (XSS) This could cker to pitrary ode in of the owser of this s user uch as	https://helpx dobe.com/se ity/products, perience- manager/aps 4-28.html	cur /ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	4.8	Scripting vulnerability could be abus a priv attacker to malicious s into vuln form	rsions earlier by a less-Site (XSS) ithat sed by rileged inject scripts erable fields.	https://helpx dobe.com/se ity/products, perience- manager/aps 4-28.html	cur /ex	A-ADO-E 200624/	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26049		
Affected Ver	sion(s): * Up to	(excluding	g) 6.5.21		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	6.1	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/145
			2024-36216		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/146

0-1

1-2

2-3

4-5

6-7

7-8

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-20769		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-20784	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/147
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/148

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	De	escription	& CVE ID		Patch		NCIIP	C ID
			for Ma Jav ex vice what to co vu	containing the vulnerable field. CVE ID: CVE-2024-26036						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Ma 6.5 Am affi ba Sc vu all ex Jav the vice Ex iss recint co cli cra su for				s://help e.com/se products ence- ager/ap e.html	ecur s/ex	ADO-E 0624/	
Improper Neutralizat ion of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are			dobe ity/p	s://help e.com/se products ence-	ecur	.DO-Е)624/	
Web Page CVSSv3 Scoring	Scale 0-1	1-2	aff 2-3	ected by	a DOM-	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-2024-26039	manager/apsb2 4-28.html	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/151

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form that triggers the vulnerability. CVE ID: CVE-2024-26053		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject into vulnerable form fields Malicious JavaScript may be executed in a victim's browser when they browser when they browser to the page containing the vulnerable field. CVE ID: CVE- 2024-26054	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/152
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/153
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. CVE ID: CVE-2024-26055		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script. CVE ID: CVE- 2024-26057	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/154
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/155

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	D	escription	& CVE ID		Patch		NCIIP	CID
('Cross-site Scripting')			vui vui alli ex Jar th vid se Ex iss in co to sp lin CV	Inerabili ow an at ecute a vaScript e contex ctim's ssion. eploitation teraction nvincing click ecially lk. VE ID:	(XSS) ty. This ty could tacker to arbitrary code in t of the browser n of this ires user , such as a victim on a crafted CVE- 58	4-28	ager/aps .html	sb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Mark Scover of the state of the	CVE ID: CVE-2024-26058 Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26060			s://helpx e.com/se oroducts, ence- ager/aps .html	cur /ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input	13-Jun-2024	5.4	Ma	Adobe Experience Manager versions 6.5.20 and earlier			s://helpx e.com/se products/	cur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	perience- manager/apsb2 4-28.html	
			CVE ID: CVE- 2024-26066		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26068	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/158

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26070	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/159
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/160

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-26071		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. CVE ID: CVE-2024-26072	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/161
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/162

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26075	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/163
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/164

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description &	CVE ID	F	Patch		NCIII	PC ID
				in a cowser prowse page the eld.					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Scripting vulnerability could be abu an attacker to malicious into vuln form Malicious JavaScript m executed	ersions earlier by a ss-Site (XSS) that sed by o inject scripts herable fields. hay be in a rowser browse page the eld. CVE-	dobe.d ity/properien	ger/aps	cur /ex	A-ADO-I 200624,	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Expension Manager version of the control of t	dobe.d ity/properien	ger/aps	cur /ex	A-ADO-I 200624,		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26081		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26082	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/167
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/168

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26083		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26085	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/169
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/170

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE-2024-26086		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26088		A-ADO-EXPE- 200624/171
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/172

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. CVE ID: CVE-2024-26089		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. CVE ID: CVE-2024-26090	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/173
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/174
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute. CVE ID: CVE-2024-26091	manager/apsb2 4-28.html	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/175

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-26092		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26093	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/176
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	Neutralizat ion of Input During Web Page Generation ('Cross-site		Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/177

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE- 2024-26095			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26110	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/178	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an 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.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/179	

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE- 2024-26111			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26113	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/180	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26114	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/181	

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26115	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/182	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-26116	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/183	
Improper Neutralizat ion of Input	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier	https://helpx.a dobe.com/secur ity/products/ex	A-ADO-EXPE- 200624/184	
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10	

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv	3	Description & CVE ID			Patch		NCIIP	C ID
During Web Page Generation ('Cross-site Scripting')				are affect reflected (Scripting vulnerabilitation vulnerable malicious JavaScript may be within thof the browser. CVE ID: 2024-261	Cross-Site (XSS) ity. If an s able to victim to URI ag a page content executed executed victim's	man 4-28	ence- ager/ap 3.html	sb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4		Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-26121			https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html		A-ADO-EXPE- 200624/185	
Improper Neutralizat ion of Input	13-Jun-2024	5.4		Adobe Experience Manager versions 6.5.20 and earlier			https://helpx.a dobe.com/secur ity/products/ex		A-ADO-EXPE- 200624/186	
During CVSSv3 Scoring	Scale 0-1	1-2	2-	are affected by a		5-6	ence-	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3		escription	& CVE ID		Patch		NCIIP	CID
Web Page Generation ('Cross-site Scripting')			S vv c c a a minimi fed M J J a e e vv w t t c c vv C C	cripting ulnerabili ould be al n attacker nalicious orm lalicious avaScript xecuted ictim's	may be in a browser browse page the field.		ager/aps .html	sb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	A M 66 aa s S S V C C aa mi iif fee M Jia e V W to C C V V C C C C C C C C C C C C C C C	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-34119		dobe ity/p perie mana	c.com/se products	cur /ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input	13-Jun-2024	5.4	Manager versions		dobe	s://helpx e.com/se products	cur	A-ADO-E 200624/		
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-34120	perience- manager/apsb2 4-28.html	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36141	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/189

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36142	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/190
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/191

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36143		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36144	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/192
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/193

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-2024-36146		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36147	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/194
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/195
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Seneration ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Seneration ('Cr	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable field. Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36149				containing the vulnerable field. CVE ID: CVE-		
Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject manager/apsb2 4-28.html	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	dobe.com/secur ity/products/ex perience- manager/apsb2	A-ADO-EXPE- 200624/196
Malicious JavaScript may be executed in a victim's browser	Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')			Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36150		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script. CVE ID: CVE- 2024-36151	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/198
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/199

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Descriptio	n & CVE ID		Patch		NCII	PC ID
			executed victim's when the to the containing vulnerable CVE ID:	victim's browser when they browse					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	6.5.20 an are affect stored Scripting vulnerabil could be a an attacked malicious	versions ad earlier ted by a Cross-Site (XSS) lity that abused by er to inject scripts rulnerable fields. may be in a browser y browse page g the e field. CVE-	dobe. ity/pi perie	ger/ap	ecur e/ex	A-ADO- 200624	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe E Manager 6.5.20 an are affect stored Scripting vulnerabil could be a an attacked malicious into v form	dobe. ity/pi perie	ger/ap	ecur e/ex	A-ADO- 200624		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36154		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36155	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/202
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/203

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36156		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36157	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/204
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/205

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36158		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/206
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/207

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36160		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36161	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/208
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/209

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36162		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/210
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/211
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36164		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36165	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/212
Improper Neutralizat ion of Input During Web Page Generation CVSSv3 Scoring	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) 3-4 4-5	https://helpx.a dobe.com/secur ity/products/ex perience-	A-ADO-EXPE- 200624/213

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	De	escription	& CVE ID		Patch		NCIIP	C ID
('Cross-site Scripting')			co an ma int for Ma Jav ex vid wl to co vu	uld be a attacked alicious to via alicious vascript ecuted etim's nen they	field.	4-28	ager/ap I.html	osb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Ac Ma 6.!. Sc vu co an ma int for Ma Jav ex vic wl to co vu	lobe Examager 5.20 and e affectored Cripting linerability uld be a attacked alicious to virus alicious vaScript ecuted ctim's nen they	cperience versions d earlier ed by a cross-Site (XSS) ity that bused by r to inject scripts alnerable fields. may be in a browser browse page the field. CVE-	http: dobe ity/perio man 4-28	s://help e.com/so oroducts ence- ager/ap e.html	ecur s/ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page	13-Jun-2024	5.4	Ma 6.5 ar	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site			s://help e.com/so products ence-	ecur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	B D	escription	& CVE ID		Patch		NCIIP	C ID
Generation ('Cross-site Scripting')			vuico am in fo M. Jar ex vie will to co vuico Vuico CV.	rm alicious vaScript ecuted ctim's hen they	to inject scripts alnerable fields may be in a browser page the field.	4-28	nager/ap 3.html	osb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	M. 6.!! arr sto Sco vu co an min fo M. Ja' exx view to co vu CV.	ripting lnerabili uld be all attacker alicious to vu rm alicious vaScript ecuted ctim's hen they the ntaining	versions I earlier ed by a ross-Site (XSS) ty that oused by to inject scripts ilnerable fields may be in a browse page the field. CVE	http dob ity/ man 4-28	e.com/so products ence- nager/ap 3.html	ecur s/ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During	13-Jun-2024	5.4	M: 6.!	Adobe Experience Manager versions 6.5.20 and earlier are affected by a			e.com/so products ence-	ecur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	3	Description & CVE ID			Patch		ı	NCIIP	CID
Web Page Generation ('Cross-site Scripting')				Scripting vulnerability could be abuted an attacker to malicious orm Malicious avaScript nexecuted	sed by o inject scripts nerable fields. hay be in a rowser prowse page the eld. CVE-	mana 4-28.	nger/aps html	sb2			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4		Scripting vulnerability could be abuted an attacker to malicious orm Malicious avaScript nexecuted	ersions earlier by a oss-Site (XSS) that used by o inject scripts nerable fields. hay be in a rowser prowse page the eld. CVE-	dobe ity/p perie	.com/se roducts, nce- nger/aps	cur /ex	A-AI 2006		XPE- 218
Improper Neutralizat ion of Input	13-Jun-2024	5.4	N	Adobe Expe Manager ve 5.5.20 and	https://helpx.a dobe.com/secur ity/products/ex			A-AI 2006		XPE- 219	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8)	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	perience- manager/apsb2 4-28.html	
			CVE ID: CVE- 2024-36172		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36173	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/220

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36174	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/221
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/222

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36175		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36176	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/223
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/224

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-2024-36177		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36178	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/225
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/226
	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

			to the page containing the vulnerable field.		
			CVE ID: CVE- 2024-36179		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36180	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/227
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/228

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction, typically in the form of convincing a victim to visit a maliciously crafted web page or to interact with a maliciously modified DOM element within the application. CVE ID: CVE- 2024-36181		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36182	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/229
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/230

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-2024-36183		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a specially crafted form. CVE ID: CVE- 2024-36184	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/231

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36185	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/232
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/233

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36186		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36187	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/234
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/235

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		N	ICIIP	CID
			containing vulnerable CVE ID: 2024-361	field. CVE-						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	6.5.20 and are affected stored Containing vulnerability of the containing vulnerable CVE ID:	Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36189 https://help dobe.com/s ity/product perience- manager/ap 4-28.html CVE ID: CVE- 2024-36189			ecur /ex	A-AD 2006		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Ex Manager 6.5.20 and are affecte DOM-based Site Scriptivulnerability vulnerability allow an attexecute JavaScript the context victim's session. Exploitation issue requires	dobe.dity/pr	ger/ap	ecur /ex	A-AD 2006			
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4	user	5-6	6-7	7-8	<u> </u>	3-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			click on a specially crafted link or to submit a form that triggers the vulnerability.	convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36191	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/238			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/239			

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36192		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36193	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/240
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/241

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36194		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36195	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/242
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/243

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Des	cription 8	& CVE ID		Patch		NCIIP	C ID
			Java exec victi whe to cont vuln	n icious Script i cuted im's b	CVE-					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Man 6.5.2 Answaffee base Scrij vuln allow executions and the victi sess Explissurinter converte conven	lager versions and series of the context in the con	y could acker to rbitrary code in for the prowser of this res user such as a victim on a crafted ubmit a triggers bility. CVE-	dobe ity/p perio man	s://help e.com/s products ence- ager/ap e.html	ecur s/ex	ADO-E 0624/	
Improper Neutralizat ion of Input During	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a			dobe	s://help e.com/se products ence-	ecur	ADO-E 0624/	
Web Page CVSSv3 Scoring	Scale 0-1	1-2	stored Cross-Site				6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	3 D	escription	& CVE ID		Patch		NCIIP	C ID
Generation ('Cross-site Scripting')			vi ccc an m in fo M Ja ex vi w tcc ccv	rm alicious vaScript xecuted ctim's hen they	to inject scripts alnerable fields may be in a browser page the field.	4-28	ager/ap 3.html	sb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	M 6. an st So vi co an in fo M Ja ex vi w to co vi	malicious scripts into vulnerable form fields. Malicious			s://help e.com/se oroducts ence- ager/ap 8.html	ecur s/ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During	13-Jun-2024	5.4	M 6.	5.20 and	versions	dobo	s://help e.com/se products ence-	ecur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3		Description	& CVE ID		Patch		NCIIP	C ID
Web Page Generation ('Cross-site Scripting')			S vv c c a a a m in fifth M J J is e e vv vv t t c c vv	cripting ulnerabili ould be al n attacker nalicious nto vu orm falicious avaScript xecuted ictim's when they o the ontaining ulnerable VE ID:	bused by to inject scripts alnerable fields. may be in a browser browse page the field. CVE-		ager/aps .html	sb2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	AA M 66 aa s S S V C C aa m iii fe M J ii e e V V V t C C V	into vulnerable form fields. Malicious			s://helpx e.com/se oroducts ence- ager/aps .html	cur /ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input	13-Jun-2024	5.4	N	.dobe Ex Ianager .5.20 and		dobe	s://helpx com/se products	cur	A-ADO-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	perience- manager/apsb2 4-28.html	
			CVE ID: CVE- 2024-36202		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36203	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/250

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36204	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/251
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/252

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36205		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-36206	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/253
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/254

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36207		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36208	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/255
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/256

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing the vulnerable field. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. CVE ID: CVE- 2024-36210	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/257
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 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	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/258

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 victim's browser. CVE ID: CVE-2024-36211		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36212	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/259
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/260
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. CVE ID: CVE-2024-36213		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36214	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/261
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/262

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36215		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36217	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/263
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/264

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-36218		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36219	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/265
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/266

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script. CVE ID: CVE-2024-36220		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE- 2024-36221	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/267
Improper Neutralizat ion of Input During Web Page Generation	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/268

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/269

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable script to execute. CVE ID: CVE- 2024-36224		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields Malicious JavaScript may be executed in a victim's browser when they browser to the page containing the vulnerable field. CVE ID: CVE- 2024-36225	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/270
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/271
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

Web Page Generation ('Cross-site Scripting') Improper Neutralizat ion of Input During Web Page Generation Web Page Generation 13-Jun-2024 Improper Neutralizat ion of Input During Web Page Generation 13-Jun-2024 Improper Neutralizat ion of Input During Web Page Generation 13-Jun-2024 Improper Neutralizat ion of Input During Web Page Generation Improper Neutralizat ion of Input During Web Page Generation Improper Neutralizat ion of Input During Improper Neutralizat ion of Inp	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Scripting (YSS) vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE 2024-36228				convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (YSS) Adobe Experience Manager versions 6.5.20 and earlier ity/products/ex perience- manager/apsb2	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Manager versions 6.5.20 and earlier Answer: are affected by a DOMbased Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/272
Scripting') vulnerability. This vulnerability could	Neutralizat ion of Input During Web Page Generation ('Cross-site	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/273

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form. CVE ID: CVE-		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/274

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36230		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. CVE ID: CVE- 2024-36231	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/275
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/276

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CV	Æ ID		Patch		NCIIP	C ID	
			when they bro	a wser owse page the						
			CVE ID: 0 2024-36232	CVE-						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	execute arbitrary of JavaScript code in the context of the victim's browser		https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html			A-ADO-E: 200624/		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	=	ions rlier by a coss- iXSS) This ould er to	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html			A-ADO-EXPE- 200624/278		
CVSSv3 Scoring	Scale 0-1	1-2	3-4 4-	5 5	5-6	6-7	7-8	8-9	9-10	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability. CVE ID: CVE-2024-36234		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script. CVE ID: CVE- 2024-36235	https://helpx.a dobe.com/secur ity/products/ex perience-manager/apsb2 4-28.html	A-ADO-EXPE-200624/279

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM- based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link. CVE ID: CVE- 2024-36236	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/280
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross- Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to	https://helpx.a dobe.com/secur ity/products/ex perience- manager/apsb2 4-28.html	A-ADO-EXPE- 200624/281

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & C	/E ID	Patch		NCIIP	C ID
			click on a malic link or to into with a malicid crafted web pa CVE ID: 2024-36238	eract ously				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024	5.4	execute arbitrary displayed arbitrary displaye		s://helpx e.com/sec products/ ence- ager/aps 8.html	cur 'ex	A-ADO-E 200624/	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	13-Jun-2024 Scale 0-1	4.8	Manager vers 6.5.20 and ea are affected l stored Cross Scripting (vulnerability could be abuse a privil attacker to i malicious so into vulner	sions arlier oy a http cobe that dobe dobe ity/p that perion d by man eged nject ripts cable elds.	s://helpx e.com/sec products/ ence- ager/aps B.html	cur 'ex	A-ADO-E 200624/	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID: CVE-2024-26049		
Vendor: app	ort_project				
Product: ap					
Affected Ver	sion(s): * Up to	(excluding			
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot CVE ID: CVE-2022-28657	N/A	A-APP-APPO- 200624/284
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections CVE ID: CVE- 2022-28655	N/A	A-APP-APPO- 200624/285
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	04-Jun-2024	5.5	~/.config/apport/s ettings parsing is vulnerable to "billion laughs" attack CVE ID: CVE- 2022-28652	N/A	A-APP-APPO- 200624/286
Allocation of Resources	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log	N/A	A-APP-APPO- 200624/287

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			CVE ID: CVE- 2022-28654		
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process CVE ID: CVE- 2022-28656	N/A	A-APP-APPO- 200624/288
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing CVE ID: CVE-	N/A	A-APP-APPO- 200624/289
Vendor: AR	M		2022-28658		
	rost_gpu_kern	el driver			
			r34p0 Up to (excludir	ng) r41p0	
Use After Free	07-Jun-2024	5.5	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory. This issue affects Bifrost GPU Kernel Driver: from r34p0 through r40p0; Valhall GPU Kernel Driver: from r34p0 through r40p0.	https://develop er.arm.com/Ar m Security Center/Mali GPU Driver Vulnerabilities	A-ARM-BIFR- 200624/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE- 2024-4610			
Product: va	lhall_gpu_kern	el_driver				
Affected Ver	sion(s): From (i	ncluding)	r34p0 Up to (excludin	ng) r41p0		
Use After Free	07-Jun-2024	5.5	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory. This issue affects Bifrost GPU Kernel Driver: from r34p0 through r40p0; Valhall GPU Kernel Driver: from r34p0 through r40p0. CVE ID: CVE-2024-4610	https://develop er.arm.com/Ar m Security Center/Mali GPU Driver Vulnerabilities	A-ARM-VALH- 200624/291	
Vendor: arv	vebdesign					
Product: da	shboard_to-do	_list				
Affected Ver	sion(s): * Up to	(excluding	g) 1.3.0			
Missing Authorizati on	10-Jun-2024	8.8	Missing Authorization vulnerability in Andrew Rapps Dashboard To-Do List.This issue affects Dashboard To-Do List: from n/a through 1.2.0.	N/A	A-ARW-DASH- 200624/292	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-35723		
Vendor: aut	hlib				
Product: au	thlib				
Affected Vers	sion(s): * Up to	(excluding	g) 1.3.1		
Improper Verificatio n of Cryptograp hic Signature	09-Jun-2024	7.5	lepture Authlib before 1.3.1 has algorithm confusion with asymmetric public keys. Unless an algorithm is specified in a jwt.decode call, HMAC verification is allowed with any asymmetric public key. (This is similar to CVE-2022-29217 and CVE-2024-33663.)	N/A	A-AUT-AUTH- 200624/293
			CVE ID: CVE- 2024-37568		
Vendor: aut	owriter				
Product: ai_	post_generato	r_\ _auto	writer		
Affected Vers	sion(s): * Up to	(excluding	g) 3.4		
Missing Authorizati on	09-Jun-2024	8.8	Missing Authorization vulnerability in AutoWriter AI Post Generator AutoWriter.This issue affects AI Post Generator AutoWriter: from n/a through 3.3. CVE ID: CVE- 2024-32713	N/A	A-AUT-AI_P- 200624/294
Vendor: Ava	ist				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: an	tivirus							
Affected Version(s): * Up to (excluding) 24.2								
Improper Link Resolution Before File Access ('Link Following')	10-Jun-2024	7	A sym-linked file accessed via the repair function in Avast Antivirus <24.2 on Windows may allow user to elevate privilege to delete arbitrary files or run processes as NT AUTHORITY\SYST EM. The vulnerability exists within the "Repair" (settings -> troubleshooting -> repair) feature, which attempts to delete a file in the current user's AppData directory as NT AUTHORITY\SYST EM. A low-privileged user can make a pseudosymlink and a junction folder and point to a file on the system. This can provide a low-privileged user an Elevation of Privilege to win a race-condition which will recreate the system files and make Windows callback to a specially-crafted file which	N/A	A-AVA-ANTI- 200624/295			

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			could be used to launch a privileged shell instance.				
			This issue affects Avast Antivirus prior to 24.2.				
			CVE ID: CVE- 2024-5102				
Vendor: aw	plife				l		
Product: im	age_gallery						
Affected Ver	sion(s): * Up to	(excluding	g) 1.4.6				
Missing Authorizati on	10-Jun-2024	8.8	Missing Authorization vulnerability in A WP Life Image Gallery - Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery.This issue affects Image Gallery - Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery, Masonry Gallery; from n/a through 1.4.5. CVE ID: CVE-	N/A	A-AWP-IMAG- 200624/296		
			2024-35721				
Product: slider_responsive_slideshow							
Affected Version(s): * Up to (excluding) 1.4.2							
Missing Authorizati on	10-Jun-2024	8.8	Missing Authorization vulnerability in A WP Life Slider Responsive Slideshow - Image slider, Gallery slideshow.This	N/A	A-AWP-SLID- 200624/297		

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Slider Responsive Slideshow – Image slider, Gallery slideshow: from n/a through 1.4.0.		
			CVE ID: CVE- 2024-35722		
Vendor: bak	ery_online_or	dering_sy	stem_project		
Product: ba	kery_online_or	dering_s	ystem		
Affected Vers	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-Jun-2024	9.8	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument txtsearch 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-267091. CVE ID: CVE-2024-5635	N/A	A-BAK-BAKE- 200624/298
Improper Neutralizat ion of	05-Jun-2024	9.8	A vulnerability was found in itsourcecode	N/A	A-BAK-BAKE- 200624/299

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Bakery Online Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file report/index.php. The manipulation of the argument procduct 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-267092. CVE ID: CVE-2024-5636		
Vendor: bey					
Product: bey		(ovalvdin	~) 22 1		
Affected vers	sion(s): * Up to	(excluding			T
N/A	04-Jun-2024	5.3	Prior to 23.1, an information disclosure vulnerability exists within BeyondInsight which can allow an attacker to enumerate usernames. CVE ID: CVE-2024-4220	https://www.b eyondtrust.com /trust- center/security- advisories/BT2 4-06	A-BEY-BEYO- 200624/300
Affected Vers	sion(s): * Up to	(excluding	g) 23.2	1	1

1-2

2-3

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)	04-Jun-2024	9.1	Prior to 23.2, it is possible to perform arbitrary Server-Side requests via HTTP-based connectors within BeyondInsight, resulting in a server-side request forgery vulnerability. CVE ID: CVE-2024-4219	https://www.b eyondtrust.com /trust- center/security- advisories/BT2 4-05	A-BEY-BEYO- 200624/301	
Vendor: Bite	defender					
Product: gra	avityzone					
	sion(s): * Up to	(excluding	g) 6.38.1-2			
Server- Side Request Forgery (SSRF)	06-Jun-2024	9.8	A host whitelist parser issue in the proxy service implemented in the GravityZone Update Server allows an attacker to cause a serverside request forgery. This issue only affects GravityZone Console versions before 6.38.1-2 that are running only on premise. CVE ID: CVE-2024-4177	N/A	A-BIT-GRAV- 200624/302	
Vendor: born05 Product: two-factor_authentication						
	sion(s): * Up to					
Improper Authentica tion	06-Jun-2024	6.5	The CraftCMS plugin Two-Factor Authentication	N/A	A-BOR-TWO 200624/303	

ly Protected Credentials 06-Jun-2024 8.1 the password hash of the currently authenticated user after submitting a valid TOTP. CVE ID: CVE 2024-5657 Vendor: bosathemes Product: bosa_elementor_addons_and_templates_for_woocommerce Affected Version(s): * Up to (excluding) 1.0.13 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi Missing A-BOS-BOSA-	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
The CraftCMS plugin Two-Factor Authentication in versions 3.3.1, 3.3.2 and 3.3.3 discloses the password hash of the currently authenticated user after submitting a valid TOTP. CVE ID: CVE_2024-5657 Vendor: bosathemes Product: bosa_elementor_addons_ad_templates_for_woocommerce Affected Version(s): * Up to (excluding) 1.0.13 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi s is suse affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12. CVE ID: CVE_2024-35724				allows reuse of TOTP tokens multiple times within the validity period. CVE ID: CVE-		
Description Description	Affected Vers	sion(s): From (i	ncluding)	3.3.1 Up to (excluding	g) 3.3.4	
Affected Version(s): * Up to (excluding) 1.0.13 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi s issue affects Bosa Elementor Addons and Templates for WooCommerce from n/a through 1.0.12. CVE ID: CVE 2024-35724 Affected Version(s): * Up to (excluding) 1.0.13 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12.	Credentials	·	8.1	plugin Two-Factor Authentication in versions 3.3.1, 3.3.2 and 3.3.3 discloses the password hash of the currently authenticated user after submitting a valid TOTP. CVE ID: CVE-	N/A	
Affected Version(s): * Up to (excluding) 1.0.13 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi s issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12. CVE ID: CVE- 2024-35724 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12.	Vendor: bos	athemes				
Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi s issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12. CVE ID: CVE- 2024-35724 Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12.	Product: bo	sa_elementor_	addons_a	nd_templates_for_we	oocommerce	
Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi s issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12. CVE ID: CVE- 2024-35724 A-BOS-BOSA- 200624/305	Affected Vers	sion(s): * Up to	(excluding	g) 1.0.13		
Vendor: brizy	Authorizati on	·		Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.Thi s issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12. CVE ID: CVE-	N/A	
	Vendor: bri	zy				

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: br	izy-page_build	er					
Affected Version(s): * Up to (excluding) 2.4.42							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post content in all versions up to, and including, 2.4.41 due to insufficient input sanitization performed only on the client side and insufficient output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-1940	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&old=305 5256%40brizy &new=3055256 %40brizy&sfp_ email=&sfph_m ail=	A-BRI-BRIZ- 200624/306		
Affected Ver	sion(s): * Up to	(excluding	g) 2.4.44				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form name values in all versions up to, and including, 2.4.43 due to insufficient input	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 86506%40brizy %2Ftrunk&old= 3058896%40br izy%2Ftrunk&s	A-BRI-BRIZ- 200624/307		
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-2087	fp_email=&sfph _mail=	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Attributes for blocks in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-1161	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 86506%40brizy %2Ftrunk&old= 3058896%40br izy%2Ftrunk&s fp_email=&sfph _mail=	A-BRI-BRIZ- 200624/308

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Link To' field of multiple widgets in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-3667	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 86506%40brizy %2Ftrunk&old= 3058896%40br izy%2Ftrunk&s fp_email=&sfph _mail=	A-BRI-BRIZ- 200624/309
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's contact form widget error message and redirect URL in all versions up to, and including, 2.4.43 due to insufficient input sanitization	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 86506%40brizy %2Ftrunk&old= 3058896%40br izy%2Ftrunk&s fp_email=&sfph _mail=	A-BRI-BRIZ- 200624/310

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			and output escaping on user supplied error messages. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
Vendor: bud	ldyboss		2024-1164			
	ddyboss_platfo	arm.				
	sion(s): * Up to		a) 2 6 NN			
Authorizati on Bypass Through User- Controlled Key	05-Jun-2024	4.3	The contains an IDOR vulnerability that allows a user to comment on a private post by manipulating the ID included in the request CVE ID: CVE-2024-4886	N/A	A-BUD-BUDD- 200624/311	
	ldypress_cove	• 1				
Product: buddypress_cover						
Affected Vers	sion(s): * Up to	lincluding		I	I	
Unrestricte d Upload of File with Dangerous Type	10-Jun-2024	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in Asghar Hatampoor BuddyPress Cover	N/A	A-BUD-BUDD- 200624/312	

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows Code Injection.This issue affects BuddyPress Cover: from n/a through 2.1.4.2. CVE ID: CVE- 2024-35746		
Vendor: Cisc	со				
Product: fin	esse				
Affected Vers	sion(s): * Up to	(excluding	g) 11.6\\(1\\)		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of usersupplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	https://sec.cloudapps.cisco.com/security/center/CiscoSecurityAdvisory/cisco-safinesse-ssrf-rfi-Um7wT8Ew	A-CIS-FINE- 200624/313
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 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 interface or access sensitive information on the affected device. CVE ID: CVE-2024-20405 A vulnerability in the web-based		
			management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system.		
Server- Side Request Forgery (SSRF)	05-Jun-2024	5.3	This vulnerability is due to insufficient validation of usersupplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. CVE ID: CVE-	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- finesse-ssrf-rfi- Um7wT8Ew	A-CIS-FINE- 200624/314
			CVE ID: CVE- 2024-20404		

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Affected Version(s): $11.6 \setminus (1 \setminus)$						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of usersupplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device. CVE ID: CVE-2024-20405	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- finesse-ssrf-rfi- Um7wT8Ew	A-CIS-FINE- 200624/315	
Server- Side Request	05-Jun-2024	5.3	A vulnerability in the web-based management	https://sec.clou dapps.cisco.com /security/cente	A-CIS-FINE- 200624/316	

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system.	r/content/Cisco SecurityAdvisor y/cisco-sa- finesse-ssrf-rfi- Um7wT8Ew	
			This vulnerability is due to insufficient validation of usersupplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device.		
			CVE ID: CVE- 2024-20404		
Affected Vers	sion(s): 12.6\\(2\\)			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- finesse-ssrf-rfi- Um7wT8Ew	A-CIS-FINE- 200624/317
CVSSv3 Scoring Scale					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conduct a stored XSS attack by exploiting an RFI vulnerability.		
			This vulnerability is due to insufficient validation of usersupplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device. CVE ID: CVE-2024-20405		
Server- Side Request Forgery (SSRF)	05-Jun-2024	5.3	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system.	https://sec.clou dapps.cisco.com /security/cente r/content/Cisco SecurityAdvisor y/cisco-sa- finesse-ssrf-rfi- Um7wT8Ew	A-CIS-FINE- 200624/318

1-2

2-3

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 due to insufficient validation of usersupplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device. CVE ID: CVE-2024-20404		
Vendor: cla	 shforwindows				
Product: cla	ısh				
Affected Ver	sion(s): From (i	ncluding)	0.1.0 Up to (including	g) 0.20.1	
Improper Authentica tion	07-Jun-2024	9.8	A vulnerability was found in Clash up to 0.20.1 on Windows. It has been declared as critical. This vulnerability affects unknown code of the component Proxy Port. The manipulation leads to improper authentication. The attack can be initiated remotely.	N/A	A-CLA-CLAS- 200624/319

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-267406 is the identifier assigned to this vulnerability. CVE ID: CVE-2024-5732		
Vendor: clo	udfoundry				
Product: cf-	• •	ncluding)	30.9.0 Up to (includin	g) 40.13.0	
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	10-Jun-2024	7.5	Improper handling of requests in Routing Release > v0.273.0 and <= v0.297.0 allows an unauthenticated attacker to degrade the service availability of the Cloud Foundry deployment if performed at scale. CVE ID: CVE-2024-22279	https://www.cl oudfoundry.org /blog/cve- 2024-22279- gorouter- denial-of- service-attack/	A-CLO-CF-D- 200624/320
	uting_release				
Affected Vers	sion(s): From (i	ncluding)	0.273.0 Up to (includi		I
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP	10-Jun-2024	7.5	Improper handling of requests in Routing Release > v0.273.0 and <= v0.297.0 allows an unauthenticated attacker to degrade	https://www.cl oudfoundry.org /blog/cve- 2024-22279- gorouter- denial-of- service-attack/	A-CLO-ROUT- 200624/321

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Smuggling') Vendor: Clu		CV33V3	the service availability of the Cloud Foundry deployment if performed at scale. CVE ID: CVE-2024-22279	Fatcii	NCIIPC ID
Product: bo					
	sion(s): * Up to	(excluding	σ) 1 1		
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	A-CLU-BOOT- 200624/322
Vendor: cod					
	widgetselem				
Affected Ver	sion(s): * Up to	(including			I
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Codeless Cowidgets – Elementor Addons allows Stored XSS.This issue affects Cowidgets – Elementor Addons:	N/A	A-COD-COWI- 200624/323

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 n/a through 1.1.1. CVE ID: CVE-2024-35782						
Vendor: codeparrots									
Product: easy_forms_for_mailchimp									
Affected Ver	sion(s): * Up to	(including	g) 6.9.0						
Insertion of Sensitive Informatio n into Log File	04-Jun-2024	7.5	Insertion of Sensitive Information into Log File vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0. CVE ID: CVE-2024-25095	N/A	A-COD-EASY- 200624/324				
Missing Authorizati on	10-Jun-2024	7.3	Missing Authorization vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0. CVE ID: CVE- 2024-35742	N/A	A-COD-EASY- 200624/325				
Vendor: Coo	depeople								
Product: wp	o_time_slots_bo	oking_fo	rm						
Affected Ver	sion(s): * Up to	(excluding	g) 1.2.12						
Missing Authorizati on	10-Jun-2024	9.8	Missing Authorization vulnerability in CodePeople WP	N/A	A-COD-WP_T- 200624/326				

CVSSv3 Scoring Scale 0-1
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.2.11. CVE ID: CVE- 2024-35735		
Vendor: cor	 tact_form_bui	lder_proj			
	ntact_form_bu				
Affected Ver	sion(s): * Up to	(including	g) 2.1.7		
Improper Restriction of Excessive Authentica tion Attempts	10-Jun-2024	5.3	Improper Restriction of Excessive Authentication Attempts vulnerability in wpdevart Contact Form Builder, Contact Widget allows Functionality Bypass.This issue affects Contact Form Builder, Contact Widget: from Na through 2.1.7. CVE ID: CVE- 2024-35747	N/A	A-CON-CONT- 200624/327
Vendor: cre	ativethemes				
Product: blo					
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation	05-Jun-2024	5.4	The Blocksy theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the custom_url parameter in all	https://themes. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=22 9705%40blocks	A-CRE-BLOC- 200624/328

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

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')			versions up to, and including, 2.0.50 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. CVE ID: CVE-2024-5439	y%2F2.0.51&ol d=228990%40b locksy%2F2.0.5 0	
Vendor: crm	neb		2021 0107		
Product: crr					
Affected Vers	sion(s): 5.2.2				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2024	7.5	SQL Injection vulnerability in CRMEB v.5.2.2 allows a remote attacker to obtain sensitive information via the getProductList function in the ProductController. php file. CVE ID: CVE-2024-36837	N/A	A-CRM-CRME- 200624/329
Vendor: cyb	erchimps				
Product: res	sponsive				
Affected Vers	sion(s): * Up to	(excluding	g) 5.0.3.1		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') 4-Jun-2024 5.4 Seponsive allows Stored XSS.This issue affects Responsive: from n/a through 5.0.3. CVE ID: CVE- 2024-35654 Product: responsive_addons Affected Version(s): * Up to (excluding) 3.0.6 The Responsive Addons - Starter Templates, Advanced Features and Customizer Settings for Responsive Theme, plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject A-CYB-RESP- 200624/330 A-CYB-RESP- 200624/331 A-CYB-RESP- 200624/331	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.0.6 The Responsive Addons - Starter Templates, Advanced Features and Customizer Settings for Responsive Theme. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access	Neutralizat ion of Input During Web Page Generation ('Cross-site	04-Jun-2024	5.4	Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CyberChimps Responsive allows Stored XSS.This issue affects Responsive: from n/a through 5.0.3. CVE ID: CVE	N/A	
The Responsive Addons – Starter Templates, Advanced Features and Customizer Settings for Responsive Theme. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access	Product: res	sponsive_addo	ns			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting') Scripting') Addons – Starter Templates, Advanced Features and Customizer Settings for Responsive Theme. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access Addons – Starter Templates, Advanced Features and Customizer Settings for Responsive Trac.wordpress. org/changeset/3094256/respo nsive-add-ons/trunk/inclu des/importers/wxr-importer/class-responsive-ready-sites-wxr-importer.php	Affected Vers	sion(s): * Up to	(excludin	g) 3.0.6		
arbitrary web	Neutralizat ion of Input During Web Page Generation ('Cross-site	05-Jun-2024	5.4	Addons – Starter Templates, Advanced Features and Customizer Settings for Responsive Theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 due to insufficient inpursanitization and output escaping This makes in possible for authenticated attackers, with Author-level access and above, to injection of the startes of th	https://plugins. trac.wordpress. org/changeset/ 3094256/respo nsive-add- ons/trunk/inclu des/importers/ wxr- importer/class- responsive- ready-sites- wxr- importer.php	
	CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

			•		NCIIPC ID				
			scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE- 2024-5222						
Vendor: cyrusimap									
Product: cyrus	s_imap								
Affected Versio	n(s): * Up to (excluding	g) 3.8.3						
Allocation of Resources Without Limits or Throttling	5-Jun-2024	6.5	Cyrus IMAP before 3.8.3 and 3.10.x before 3.10.0-rc1 allows authenticated attackers to cause unbounded memory allocation by sending many LITERALs in a single command. CVE ID: CVE- 2024-34055	https://github.c om/cyrusimap/ cyrus- imapd/commit/ ef9e4e8314d6a 06f2269af0ccf6 06894cc3fe489	A-CYR-CYRU- 200624/332				
Affected Versio	n(s): 3.10.0								
Allocation of Resources Without Limits or Throttling	95-Jun-2024	6.5	Cyrus IMAP before 3.8.3 and 3.10.x before 3.10.0-rc1 allows authenticated attackers to cause unbounded memory allocation by sending many LITERALs in a single command. CVE ID: CVE- 2024-34055	https://github.c om/cyrusimap/ cyrus- imapd/commit/ ef9e4e8314d6a 06f2269af0ccf6 06894cc3fe489	A-CYR-CYRU- 200624/333				
Vendor: dexta	z_ping_proje	ct			<u></u>				
Product: dexta									

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): * Up to	(including	g) 0.65		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	04-Jun-2024	7.2	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in dexta Dextaz Ping allows Command Injection.This issue affects Dextaz Ping: from n/a through 0.65.	N/A	A-DEX-DEXT- 200624/334
	_		CVE ID: CVE- 2024-34792		
Vendor: dre	ryk				
Product: gal	binet				
Affected Vers	sion(s): From (i	ncluding)	7.0.0.0 Up to (excludi	ng) 9.17.0.0	
Use of Hard- coded Credentials	10-Jun-2024	9.8	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all drEryk Gabinet installations. This issue affects drEryk Gabinet software versions from 7.0.0.0 through 9.17.0.0.	N/A	A-DRE-GABI- 200624/335
			CVE ID: CVE- 2024-3699		
Vendor: dul	ldusk				
Product: ph	pfilemanager				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 1.7.8			L	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	6.1	Vulnerability in Dulldusk's PHP File Manager affecting version 1.7.8. This vulnerability consists of an XSS through the fm_current_dir parameter of index.php. An attacker could send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session. CVE ID: CVE-2024-5673	N/A	A-DUL-PHPF- 200624/336
Vendor: ele	arningfreak				
Product: ins	sert_or_embed	_articulat	te_content		
Affected Ver	sion(s): * Up to	(including	g) 4.3000000023		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	The Insert or Embed Articulate Content into WordPress plugin through 4.3000000023 lacks validation of URLs when adding iframes, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page. CVE ID: CVE-	N/A	A-ELE-INSE- 200624/337
			2024-0756		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: em	ailgpt				
Affected Vers	sion(s): -				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	05-Jun-2024	9.1	The EmailGPT service contains a prompt injection vulnerability. The service uses an API service that allows a malicious user to inject a direct prompt and take over the service logic. Attackers can exploit the issue by forcing the AI service to leak the standard hard-coded system prompts and/or execute unwanted prompts. When engaging with EmailGPT by submitting a malicious prompt that requests harmful information, the system will respond by providing the requested data. This vulnerability can be exploited by any individual with access to the service. CVE ID: CVE-2024-5184	N/A	A-EMA-EMAI- 200624/338
Product: em					
Affected vers	sion(s): 2.3.0	1-2 2	!- 3 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)	10-Jun-2024	6.5	Emlog pro2.3 is vulnerable to Cross Site Request Forgery (CSRF) via twitter.php which can be used with a XSS vulnerability to access administrator information. CVE ID: CVE-2024-31612	N/A	A-EML-EMLO- 200624/339	
Vendor: env	othemes					
Product: en						
Affected Ver	sion(s): * Up to	(excluding				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Envo Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_css_id' parameter within the Button widget in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins. trac.wordpress. org/changeset/ 3098500/	A-ENV-ENVO- 200624/340	

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-5645		
Vendor: env	oyproxy				
Product: en	voy				
Affected Ver	sion(s): * Up to	(excluding	g) 1.27.6		
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	04-Jun-2024	8.2	Envoy is a cloud- native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc- editor.org/rfc/rfc7 230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response.	https://github.c om/envoyproxy /envoy/security /advisories/GH SA-vcf8-7238- v74c	A-ENV-ENVO- 200624/341

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-23326		
Use After Free	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. A crash was observed in 'EnvoyQuicServerS tream::OnInitialHe adersComplete()' with following call stack. It is a use- after-free caused by QUICHE continuing push request headers after 'StopReading()' being called on the stream. As after 'StopReading()', the HCM's 'ActiveStream' might have already be destroyed and any up calls from QUICHE could potentially cause use after free.	N/A	A-ENV-ENVO- 200624/342
			2024-32974		
Integer Underflow (Wrap or Wraparoun d)	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. There is a crash at 'QuicheDataReader ::PeekVarInt62Len gth()'. It is caused by integer underflow in the 'QuicStreamSeque ncerBuffer::PeekRe		A-ENV-ENVO- 200624/343
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7	-8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			gion()` implementation. CVE ID: CVE- 2024-32975				
Out-of- bounds Write	04-Jun-2024	6.5	exposed an out-of-memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer.	ative, open source lige and service loxy. Envoy sposed an out-of-emory (OOM) ector from the irror response, nice async HTTP lent will buffer e response with a unbounded affer. VE ID: CVE-D24-34364 Invoy is a cloud-			
Use After Free	04-Jun-2024	5.9	Envoy is a cloud- native, open source edge and service proxy. There is a use-after-free in 'HttpConnectionMa nager' (HCM) with 'EnvoyQuicServerS tream' that can crash Envoy. An attacker can exploit this vulnerability by sending a request without 'FIN', then a 'RESET_STREAM' frame, and then after receiving the response, closing the connection. CVE ID: CVE- 2024-34362	N/A	A-ENV-ENVO- 200624/345		
Affected Ver	sion(s): From (i	ncluding)	1.18.0 Up to (excludi	ng) 1.27.6	·		
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7	-8 8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Loop with Unreachabl e Exit Condition ('Infinite Loop')	04-Jun-2024	con(s): From (including) 1.28		N/A	A-ENV-ENVO- 200624/346	
Affected Ver	sion(s): From (i	ncluding)		ng) 1.28.4		
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	04-Jun-2024	8.2	Envoy is a cloud- native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc- editor.org/rfc/rfc7 230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be	https://github.c om/envoyproxy /envoy/security /advisories/GH SA-vcf8-7238- v74c	A-ENV-ENVO- 200624/347	

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tricked into adding the upgrade header to the response. CVE ID: CVE-2024-23326		
Use After Free	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. A crash was observed in 'EnvoyQuicServerS tream::OnInitialHe adersComplete()' with following call stack. It is a use- after-free caused by QUICHE continuing push request headers after 'StopReading()' being called on the stream. As after 'StopReading()', the HCM's 'ActiveStream' might have already be destroyed and any up calls from QUICHE could potentially cause use after free. CVE ID: CVE- 2024-32974	N/A	A-ENV-ENVO- 200624/348
Integer Underflow (Wrap or Wraparoun d)	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. There is a crash at 'QuicheDataReader	N/A	A-ENV-ENVO- 200624/349
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			::PeekVarInt62Len gth()`. It is caused by integer underflow in the `QuicStreamSeque ncerBuffer::PeekRe gion()` implementation. CVE ID: CVE-2024-32975		
Loop with Unreachabl e Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input. CVE ID: CVE- 2024-32976	N/A	A-ENV-ENVO- 200624/350
N/A	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception would cause Envoy to crash. CVE ID: CVE- 2024-34363	N/A	A-ENV-ENVO- 200624/351

CVSSv3 Scoring Scale	0-1	1-2	2-3	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	04-Jun-2024	6.5	Envoy is a cloud- native, open source edge and service proxy. Envoy exposed an out-of- memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. CVE ID: CVE- 2024-34364	N/A	A-ENV-ENVO- 200624/352
Use After Free	04-Jun-2024	5.9	Envoy is a cloud- native, open source edge and service proxy. There is a use-after-free in 'HttpConnectionMa nager' (HCM) with 'EnvoyQuicServerS tream' that can crash Envoy. An attacker can exploit this vulnerability by sending a request without 'FIN', then a 'RESET_STREAM' frame, and then after receiving the response, closing the connection. CVE ID: CVE- 2024-34362	N/A	A-ENV-ENVO- 200624/353
Affected Ver	sion(s): From (i	ncluding)	1.29.0 Up to (excluding	ng) 1.29.5	
Inconsiste nt Interpretat ion of	04-Jun-2024	8.2	Envoy is a cloud- native, open source edge and service proxy. A theoretical	https://github.c om/envoyproxy /envoy/security /advisories/GH	A-ENV-ENVO- 200624/354

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description	& CVE ID	Р	atch		NCIIP	CID
HTTP Requests ('HTTP Request Smuggling')			tricked into an upgrade into a responsive process. Incorrectly a 200 r from a server requesting protocol and the column of the c	ty exists avoy if a an be o adding header onse. Per overfc-rfc/rfc7 n-6.7 a and 101 witching Envoy accepts response wer when a supgrade, loes not protocol is opens sibility of nuggling and be o adding the header	SA-vcf8 v74c	3-7238-			
			CVE ID: 2024-2332	CVE-					
Use After Free	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerS tream::OnInitialHe adersComplete()` with following call stack. It is a use-			A-ENV-E 200624/			
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free caused by QUICHE continuing push request headers after 'StopReading()' being called on the stream. As after 'StopReading()', the HCM's 'ActiveStream' might have already be destroyed and any up calls from QUICHE could potentially cause use after free.		
			CVE ID: CVE- 2024-32974		
Integer Underflow (Wrap or Wraparoun d)	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. There is a crash at 'QuicheDataReader ::PeekVarInt62Len gth()'. It is caused by integer underflow in the 'QuicStreamSeque ncerBuffer::PeekRe gion()' implementation. CVE ID: CVE- 2024-32975	N/A	A-ENV-ENVO- 200624/356
Loop with Unreachabl e Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during	N/A	A-ENV-ENVO- 200624/357

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decompression of Brotli data with extra input. CVE ID: CVE- 2024-32976		
N/A	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception would cause Envoy to crash. CVE ID: CVE- 2024-34363	N/A	A-ENV-ENVO- 200624/358
Out-of- bounds Write	04-Jun-2024	6.5	Envoy is a cloud- native, open source edge and service proxy. Envoy exposed an out-of- memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. CVE ID: CVE- 2024-34364	N/A	A-ENV-ENVO- 200624/359
Use After Free	04-Jun-2024	5.9	Envoy is a cloud- native, open source edge and service proxy. There is a	N/A	A-ENV-ENVO- 200624/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free in 'HttpConnectionMa nager' (HCM) with 'EnvoyQuicServerS tream' that can crash Envoy. An attacker can exploit this vulnerability by sending a request without 'FIN', then a 'RESET_STREAM' frame, and then after receiving the response, closing the connection. CVE ID: CVE- 2024-34362		
Affected Ver	sion(s): From (i	ncluding)	1.30.0 Up to (excluding	ng) 1.30.2	
Inconsiste nt Interpretat ion of HTTP Requests ('HTTP Request Smuggling')	04-Jun-2024 Scale 0-1	8.2	Envoy is a cloud- native, open source edge and service proxy. A theoretical request smuggling vulnerability exists through Envoy if a server can be tricked into adding an upgrade header into a response. Per RFC https://www.rfc- editor.org/rfc/rfc7 230#section-6.7 a server sends 101 when switching protocols. Envoy incorrectly accepts a 200 response from a server when requesting a protocol upgrade, but 200 does not	https://github.c om/envoyproxy /envoy/security /advisories/GH SA-vcf8-7238- v74c	A-ENV-ENVO- 200624/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			indicate protocol switch. This opens up the possibility of request smuggling through Envoy if the server can be tricked into adding the upgrade header to the response.		
			CVE ID: CVE- 2024-23326		
Use After Free	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. A crash was observed in `EnvoyQuicServerS tream::OnInitialHe adersComplete()` with following call stack. It is a use- after-free caused by QUICHE continuing push request headers after `StopReading()` being called on the stream. As after `StopReading()`, the HCM's `ActiveStream` might have already be destroyed and any up calls from QUICHE could potentially cause use after free. CVE ID: CVE- 2024-32974	N/A	A-ENV-ENVO- 200624/362
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. There is a crash at 'QuicheDataReader ::PeekVarInt62Len gth()'. It is caused by integer underflow in the 'QuicStreamSeque ncerBuffer::PeekRe gion()' implementation. CVE ID: CVE- 2024-32975	N/A	A-ENV-ENVO- 200624/363
Loop with Unreachabl e Exit Condition ('Infinite Loop')	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. Envoyproxy with a Brotli filter can get into an endless loop during decompression of Brotli data with extra input. CVE ID: CVE- 2024-32976	N/A	A-ENV-ENVO- 200624/364
N/A	04-Jun-2024	7.5	Envoy is a cloud- native, open source edge and service proxy. Due to how Envoy invoked the nlohmann JSON library, the library could throw an uncaught exception from downstream data if incomplete UTF-8 strings were serialized. The uncaught exception	N/A	A-ENV-ENVO- 200624/365

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			would cause Envoy to crash. CVE ID: CVE-2024-34363				
Out-of- bounds Write	04-Jun-2024	6.5	Envoy is a cloud- native, open source edge and service proxy. Envoy exposed an out-of- memory (OOM) vector from the mirror response, since async HTTP client will buffer the response with an unbounded buffer. CVE ID: CVE- 2024-34364	N/A	A-ENV-ENVO- 200624/366		
Use After Free	04-Jun-2024	5.9	Envoy is a cloud- native, open source edge and service proxy. There is a use-after-free in 'HttpConnectionMa nager' (HCM) with 'EnvoyQuicServerS tream' that can crash Envoy. An attacker can exploit this vulnerability by sending a request without 'FIN', then a 'RESET_STREAM' frame, and then after receiving the response, closing the connection. CVE ID: CVE- 2024-34362	N/A	A-ENV-ENVO- 200624/367		
Vendor: estomed							
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Product: sin	nple_care					
Affected Vers	sion(s): *					
Use of Hard- coded Credentials	10-Jun-2024	9.8	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Simple Care software installations. This issue affects Estomed Sp. z o.o. Simple Care software in all versions. The software is no longer supported. CVE ID: CVE-2024-3700	N/A	A-EST-SIMP- 200624/368	
Vendor: eur	osoft					
Product: pr	zychodnia					
Affected Vers	sion(s): * Up to	(excluding	g) 20240417.001			
Use of Hard- coded Credentials	10-Jun-2024	9.8	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Eurosoft Przychodnia installations.	N/A	A-EUR-PRZY- 200624/369	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description &	CVE ID		Patch		NCIIF	CID
			vulnerability fixed). CVE ID:	on 202 (from version					
Vendor: ext	andthamas		2024-1228						
	libri_page_buil	der							
	sion(s): * Up to		g) 1.0.277						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	Scripting viplugin's shortcode(s) versions up tincluding, 1 due to insufinput saniti	is to is ses-Site a the in all to, and l.0.276 fficient ization output a user ibutes. Les it for d with evel above, bitrary ts in will never a es an	trac.v	://plugi vordpre hangeso	ess.	A-EXT-C 200624/	
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-5038		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's colibri_video_playe r shortcode in all versions up to, and including, 1.0.276 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4451	https://plugins. trac.wordpress. org/changeset/ 3097694/colibr i-page- builder/trunk/e xtend- builder/shortco des/video.php	A-EXT-COLI- 200624/371
Vendor: file	organizer			l	1
Product: file	eorganizer				
Affected Ver	sion(s): * Up to	(excludin	g) 1.0.8		
N/A	07-Jun-2024	7.5	The FileOrganizer – Manage WordPress and Website Files plugin for WordPress is vulnerable to Sensitive	https://plugins. trac.wordpress. org/changeset/ 3098763/	A-FIL-FILE- 200624/372
CVSSv3 Scoring	Scale 0-1	1-2 2	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 Exposure in all versions up to, and including, 1.0.7 via the 'fileorganizer_ajax_ handler' function. This makes it possible for unauthenticated attackers to extract sensitive data including backups or other sensitive information if the files have been moved to the built-in Trash folder. CVE ID: CVE-2024-5599		
Vendor: five	estarplugins				
	e_star_restaur	ant_ment	1		
Affected Ver	sion(s): * Up to	(excluding	g) 2.4.17		
Missing Authorizati on	05-Jun-2024	4.3	The Restaurant Menu and Food Ordering plugin for WordPress is vulnerable to unauthorized creation of data due to a missing capability check on 'add_section', 'add_menu', 'add_menu_item', and 'add_menu_page' functions in all versions up to, and including, 2.4.16. This makes it possible for	https://plugins. trac.wordpress. org/changeset/ 3097599/	A-FIV-FIVE- 200624/373

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attackers, with Subscriber-level access and above, to create menu sections, menus, food items, and new menu pages. CVE ID: CVE- 2024-5459		
Vendor: for	mwork_projec	t			1
Product: for	mwork				
Affected Vers	sion(s): * Up to	(excludin	g) 1.13.1		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	4.8	Formwork is a flat file-based Content Management System (CMS). An attackers (requires administrator privilege) to execute arbitrary web scripts by modifying site options via /panel/options/sit e. This type of attack is suitable for persistence, affecting visitors across all pages (except the dashboard). This vulnerability is fixed in 1.13.1. CVE ID: CVE-2024-37160	https://github.c om/getformwor k/formwork/co mmit/9d47120 4f7ebb51c3c27 131581c2b834 315b5e0b, https://github.c om/getformwor k/formwork/co mmit/f5312015 a5a5e89b95ef2 bd07e496f8474 d579c5	A-FOR-FORM- 200624/374
Vendor: For	tinet				
Product: for	tiwebmanage	r			
Affected Vers	sion(s): 6.0.2				

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Authorizati on	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. CVE ID: CVE-2024-23669	https://fortigua rd.fortinet.com/ psirt/FG-IR-23- 222	A-FOR-FORT- 200624/375
Affected Ver	sion(s): 6.3.0				
Incorrect Authorizati on	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. CVE ID: CVE-2024-23669	https://fortigua rd.fortinet.com/ psirt/FG-IR-23- 222	A-FOR-FORT- 200624/376
Affected Ver	sion(s): 7.2.0				
Incorrect Authorizati on	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and	https://fortigua rd.fortinet.com/ psirt/FG-IR-23- 222	A-FOR-FORT- 200624/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. CVE ID: CVE-2024-23669 6.2.3 Up to (excluding	g) 6.2.5	
Incorrect Authorizati on	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI. CVE ID: CVE-2024-23669	https://fortigua rd.fortinet.com/ psirt/FG-IR-23- 222	A-FOR-FORT- 200624/378
Affected Ver	sion(s): From (i	ncluding)	7.0.0 Up to (excluding	g) 7.0.5	
Incorrect Authorizati on	05-Jun-2024	8.8	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	https://fortigua rd.fortinet.com/ psirt/FG-IR-23- 222	A-FOR-FORT- 200624/379

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Desc	ription	& CVE ID		Patch		NCIIP	CID
			CVE 2024	ID: 1-236	CVE-					
Vendor: fuji	electric									
Product: mo	onitouch_v-sft									
Affected Ver	sion(s): * Up to	(excludin	g) 6.2.	3.0						
Access of Resource Using Incompatib le Type ('Type Confusion')	10-Jun-2024	9.8	vulne confi could or co	erable usion, d caus	e a crash ecution. CVE-	N/A			A-FUJ-M0 200624/	
Vendor: gai	zhenbiao									
Product: ch	uanhuchatgpt									
Affected Ver	sion(s): * Up to	(includin	g) 202	40410)					
N/A	04-Jun-2024	7.5	contivulne in gaizh huch applis spectors allow the stany with any interbetw Exployed breathe the	rol erabili erabili nenbia atgpt icatior ifically on 20 vulr vs any erver chat h othe out raction reen ti oitatio erabili to ches, i expo itive	in 240410. Decay of the users of the users of this data including	N/A			A-GAI-CF 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	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, or confidential conversations. Additionally, it could facilitate identity theft and manipulation or fraud through the unauthorized access to users' chat histories. This issue is due to insufficient access control mechanisms in the application's handling of chat history data. CVE ID: CVE-2024-4520		
Vendor: gan	ninress		2024-4520		
	mipresslink				
	sion(s): * Up to		g) 1.1.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The GamiPress – Link plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's gamipress_link shortcode in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 96646%40gami press- link%2Ftrunk& old=2989725% 40gamipress- link%2Ftrunk& sfp_email=&sfp h_mail=	A-GAM-GAMI- 200624/382

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-5536		
Vendor: gen	eratepress				
Product: ger					
Affected Vers	sion(s): * Up to	(excludin _i			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	6.1	The GP Premium plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the message parameter in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. CVE ID: CVE-2024-3469	N/A	A-GEN-GENE- 200624/383
Vandar: gat	awesomesupp	ort		•	

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description &	CVE ID		Patch		NCIII	PCID
Product: aw	esome_suppoi	rt							
Affected Vers	sion(s): * Up to	(excludin	g) 6.1.8						
Missing Authorizati on	10-Jun-2024	8.8	Support.This affects Awe Support: from through 6.1.7	in apport esome issue esome n/a	t e N/A			A-GET-A 200624,	
			CVE ID: 2024-35741	CVE-					
Vendor: get	brave								
Product: bra	ave								
Affected Ver	sion(s): * Up to	(including	g) 0.6.9						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	4.8	Input During Page Gene (XSS or 'Cros Scripting') vulnerability Brave Brave B Builder a Stored XS issue affects Popup Bu	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brave Brave Popup Builder allows Stored XSS.This issue affects Brave Popup Builder: from n/a through 0.6.9. CVE ID: CVE-			A-GET-E 200624,		
Vendor: get	shortcodes								
Product: sh	ortcodes_ultim	ate							
Affected Vers	sion(s): * Up to	(excludin	g) 7.1.7						
Improper Neutralizat ion of Input During Web Page	05-Jun-2024	5.4	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is		trac.v org/o	://plug wordpre changes mail=&s il=&rep	ess. et? sfp	A-GET-S 200624,	
CVSSv3 Scoring	Scale 0-1	1-2 2	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')			vulnerable to Stored Cross-Site Scripting via the plugin's su_lightbox shortcode in all versions up to, and including, 7.1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4821	ame=&new=30 96024%40shor tcodes- ultimate%2Ftru nk&old=308416 2%40shortcode s- ultimate%2Ftru nk&sfp_email= &sfph_mail=#fil e1	
Vendor: Go	lang			l	1
Product: go					
Affected Ver	sion(s): * Up to	(excludin	g) 1.21.11		
N/A	05-Jun-2024	9.8	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false for addresses which would return true in their traditional IPv4 forms. CVE ID: CVE-2024-24790	https://go.dev/ cl/590316	A-GOL-GO- 200624/387

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	5.5	The archive/zip package's handling of certain types of invalid zip files differs from the behavior of most zip implementations. This misalignment could be exploited to create an zip file with contents that vary depending on the implementation reading the file. The archive/zip package now rejects files containing these errors. CVE ID: CVE-2024-24789	https://go.dev/ cl/585397, https://go.dev/i ssue/66869	A-GOL-GO- 200624/388
Affected Ver	sion(s): From (i	ncluding)	1.22.0 Up to (excludir	ng) 1.22.4	
N/A	05-Jun-2024	9.8	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false for addresses which would return true in their traditional IPv4 forms. CVE ID: CVE-	https://go.dev/ cl/590316	A-GOL-GO- 200624/389
			CVE ID: CVE- 2024-24790		
N/A	05-Jun-2024	5.5	The archive/zip package's handling of certain types of invalid zip files differs from the	https://go.dev/ cl/585397, https://go.dev/i ssue/66869	A-GOL-GO- 200624/390

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior of most zip implementations. This misalignment could be exploited to create an zip file with contents that vary depending on the implementation reading the file. The archive/zip package now rejects files containing these errors.		
			CVE ID: CVE- 2024-24789		
Vendor: gra	fana				
Product: on	call				
Affected Ver	sion(s): From (i	ncluding)	1.1.37 Up to (excluding	ng) 1.5.2	
Server- Side Request Forgery (SSRF)	05-Jun-2024	9.1	Grafana OnCall is an easy-to-use oncall management tool that will help reduce toil in oncall management through simpler workflows and interfaces that are tailored specifically for engineers. Grafana OnCall, from version 1.1.37 before 1.5.2 are vulnerable to a Server Side Request Forgery (SSRF)	https://grafana.com/security/security-advisories/cve-2024-5526/	A-GRA-ONCA- 200624/391

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webhook functionallity.		
			This issue was fixed in version 1.5.2		
			CVE ID: CVE- 2024-5526		
Vendor: hor	nebrew				
Product: jar	1				
Affected Ver	sion(s): 0.4.12				
Unrestricte d Upload of File with Dangerous Type	04-Jun-2024	9.8	An arbitrary file upload vulnerability in the /v1/app/writeFile Sync interface of Jan v0.4.12 allows attackers to execute arbitrary code via uploading a crafted file.	N/A	A-HOM-JAN- 200624/392
			CVE ID: CVE- 2024-36858		
Unrestricte d Upload of File with Dangerous Type	04-Jun-2024	9.8	An arbitrary file upload vulnerability in the /v1/app/appendFi leSync interface of Jan v0.4.12 allows attackers to execute arbitrary code via uploading a crafted file.	N/A	A-HOM-JAN- 200624/393
			CVE ID: CVE- 2024-37273		
N/A	04-Jun-2024	7.5	Jan v0.4.12 was discovered to contain an arbitrary file read vulnerability via the	N/A	A-HOM-JAN- 200624/394

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			/v1/app/readFileS ync interface. CVE ID: CVE-					
			2024-36857					
Vendor: horea_radu								
Product: on	e_page_expres	s_compai	nion					
Affected Vers	sion(s): * Up to	(excluding	g) 1.6.38					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The One Page Express Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's one_page_express_contact_form shortcode in all versions up to, and including, 1.6.37 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4703	https://plugins. trac.wordpress. org/changeset/ 3097699/one- page-express- companion	A-HOR-ONE 200624/395			
Vendor: iceg								
Product: em	ail_subscriber	's_\&_nev	vsletters					
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-	-8 8-9 9-1 0			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): * Up to	(excludin	g) 5.7.21		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2024	9.8	The Email Subscribers by Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'hash' parameter in all versions up to, and including, 5.7.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. CVE ID: CVE-2024-4295	https://plugins. trac.wordpress. org/changeset/ 3090845/email - subscribers/tru nk/lite/includes /db/class-es- db-lists- contacts.php	A-ICE-EMAI- 200624/396
Vendor: idc	cms				
Product: ide	ccms				
Affected Vers	sion(s): 1.35				
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component	N/A	A-IDC-IDCC- 200624/397
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			admin/vpsClass_de al.php?mudi=add CVE ID: CVE-				
			2024-36547				
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/vpsCompan y_deal.php?mudi=d el	N/A	A-IDC-IDCC- 200624/398		
			CVE ID: CVE- 2024-36548				
Cross-Site Request Forgery (CSRF)	04-Jun-2024	8.8	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompa ny_deal.php?mudi= rev&nohrefStr=clo se CVE ID: CVE-2024-36549	N/A	A-IDC-IDCC- 200624/399		
Cross-Site Request Forgery (CSRF) 04-Jun-2024 8.8 idccms V1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/vpsCompa ny_deal.php?mudi= add&nohrefStr=clo se CVE ID: CVE-2024-36550 CVE-2024-36							
Vendor: ipages_flipbook_project							
_	ages_flipbook						
Affected Vers	sion(s): * Up to	(<mark>excludi</mark> n	g) 1.5.2				

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Authorizati on	10-Jun-2024	7.3	Missing Authorization vulnerability in Avirtum iPages Flipbook.This issue affects iPages Flipbook: from n/a through 1.5.1. CVE ID: CVE- 2024-4744	N/A	A-IPA-IPAG- 200624/401
Vendor: Jetl	brains				
Product: aq	ua				
	sion(s): * Up to	(excluding	g) 2024.1.2		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.3.5, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.2.7, 2023.3.7, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-AQUA- 200624/402

CVSSv3 Scoring Scale
* stands for all versions

1-2

3-4 4-5

5-6

6-7

7-8

8-9

9-10

	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: clion				EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7,		
Affected Version(s): * Up to (excluding) 2023.1.7 GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: Intellij IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.1.7, 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, Interpretation of the properties of the propertie						
Insufficient ly Protected Credentials 10-Jun-2024 7.5 GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: Intellij IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, GoLa						
Insufficient ly Protected Credentials 10-Jun-2024 7.5 The could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: Intellij IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, GoLa	Affected Ver	sion(s): * Up to	(excluding	g) 2023.1.7	Ţ	
	ly Protected	10-Jun-2024	7.5	token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	tbrains.com/pri vacy- security/issues-	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4		
			CVE ID: CVE- 2024-37051		
Affected Vers	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.4	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-CLIO- 200624/404
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

		2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5,		
		2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
ion(s): From (i	ncluding)	2023.3.0 Up to (exclu	ding) 2023.3.5	
10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-CLIO- 200624/405
		10-Jun-2024 7.5	2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051 on(s): From (including) 2023.3.0 Up to (excluding) 2023.3.0 Up	2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4	Patch	NCIIPC ID
			CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.3	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-CLIO- 200624/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7,		
			2024.1.3, 2024.2		
			EAP3; Aqua		
			2024.1.2; CLion		
			2023.1.7, 2023.2.4,		
			2023.3.5, 2024.1.3,		
			2024.2 EAP2;		
			DataGrip 2023.1.3,		
			2023.2.4, 2023.3.5,		
			2024.1.4; DataSpell		
			2023.1.6, 2023.2.7,		
			2023.3.6, 2024.1.2,		
			2024.2 EAP1;		
			GoLand 2023.1.6,		
			2023.2.7, 2023.3.7,		
			2024.1.3, 2024.2		
			EAP3; MPS		
			2023.2.1, 2023.3.1,		
			2024.1 EAP2;		
			PhpStorm 2023.1.6,		
			2023.2.6, 2023.3.7,		
			2024.1.3, 2024.2		
			EAP3; PyCharm		
			2023.1.6, 2023.2.7,		
			2023.3.6, 2024.1.3,		
			2024.2 EAP2; Rider		
			2023.1.7, 2023.2.5,		
			2023.3.6, 2024.1.3;		
			RubyMine		
			2023.1.7, 2023.2.7,		
			2023.3.7, 2024.1.3,		
			2024.2 EAP4;		
			RustRover		
			2024.1.1;		
			WebStorm		
			2023.1.6, 2023.2.7,		
			2023.3.7, 2024.1.4		
			CVE ID: CVE-		
			2024-37051		
Product: da	tagrip				
Affected Ver	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.4	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; RustRover 2023.1.7, 2023.2.5, 2023.3.7, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.7, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/407

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Afforted Von	cion (c). Evore (i	and dia co	2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051	din c) 2022 2 F	
Insufficient ly Protected Credentials	sion(s): From (i	ncluding) 7.5	2024-37051 2023.3.0 Up to (exclusion could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/408
		2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,			

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051 2023.1.0 Up to (exclu	ding) 2023.1.3	
			GitHub access token could be		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	exposed to third- party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/409

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.4	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4		
Product: da	taspell		CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): * Up to	(excludin	g) 2023.1.6		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.3; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.je tbrains.com/pri vacy- security/issues-	A-JET-DATA- 200624/411
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

^{*} stands for all versions

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.7	
Insufficient ly Protected Credentials	10-Jun-2024 Scale 0-1	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.5,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2023.3.0 Up to (exclu	ding) 2023.3.6	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
weakness	Publish Date	CVSSV3	2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3; RubyMine 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3; RubyMine 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3; RubyMine 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3	Patch	NCIIPC ID
			CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.2	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-DATA- 200624/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			IDEA 2023.1.7,			
			2023.2.7, 2023.3.7,			
			2024.1.3, 2024.2			
			EAP3; Aqua			
			2024.1.2; CLion			
			2023.1.7, 2023.2.4,			
			2023.3.5, 2024.1.3,			
			2024.2 EAP2;			
			DataGrip 2023.1.3,			
			2023.2.4, 2023.3.5,			
			2024.1.4; DataSpell			
			2023.1.6, 2023.2.7,			
			2023.3.6, 2024.1.2,			
			2024.2 EAP1;			
			GoLand 2023.1.6,			
			2023.2.7, 2023.3.7,			
			2024.1.3, 2024.2			
			EAP3; MPS			
			2023.2.1, 2023.3.1,			
			2024.1 EAP2;			
			PhpStorm 2023.1.6,			
			2023.2.6, 2023.3.7,			
			2024.1.3, 2024.2			
			EAP3; PyCharm			
			2023.1.6, 2023.2.7,			
			2023.3.6, 2024.1.3,			
			2024.2 EAP2; Rider			
			2023.1.7, 2023.2.5,			
			2023.3.6, 2024.1.3;			
			RubyMine			
			2023.1.7, 2023.2.7,			
			2023.3.7, 2024.1.3,			
			2024.2 EAP4;			
			RustRover			
			2024.1.1;			
			WebStorm			
			2023.1.6, 2023.2.7,			
			2023.3.7, 2024.1.4			
			CVE ID: CVE-			
			2024-37051			
Product: goland						
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.3						

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; RyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.5, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-GOLA- 200624/415

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051					
Affected Ver	Affected Version(s): * Up to (excluding) 2023.1.6							
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.1 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; RubyMine 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2023.2.7, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2023.2.7, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2023.2.7, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.2.7, 2023.3.7, 2023.2.7, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-GOLA- 200624/416			

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-		
			2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.7	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-GOLA- 200624/417

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2023.3.0 Up to (exclu	ding) 2023.3.7	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-GOLA- 200624/418

Weakness	Publish Date	CVSSv3	Description	& CVE ID	Patc	h	NCIIP	CID
			2023.2.6, 2 2024.1.3, EAP3; E 2023.1.6, 2 2023.3.6, 2 2024.2 EAF 2023.1.7, 2 2023.3.6, 2 RubyMine 2023.1.7, 2 2023.3.7, 2 2024.2 RustRover 2024.1.1; WebStorm 2023.1.6, 2 2023.3.7, 2	2024.2 PyCharm 2023.2.7, 2024.1.3, P2; Rider 2023.2.5, 2024.1.3; 2023.2.7, 2024.1.3, EAP4;				
Product: int	ellij_idea		CVE ID: 2024-3705	CVE-				
Affected Ver	sion(s): * Up to	(excludin	g) 2023.1.7					
Insufficient ly Protected Credentials	10-Jun-2024	7.5	exposed to party sit JetBrains III version 202 less than: IDEA 2 2023.2.7, 2 2024.1.3, EAP3; 2024.1.2; 2023.3.5, 2 2024.2 DataGrip 2 2023.2.4, 2 2024.1.4; E 2023.1.6, 2 2024.2	tes in DEs after 23.1 and IntelliJ 2023.1.7, 2024.2 Aqua CLion 2023.2.4, 2024.1.3, EAP2; 2023.1.3, 2023.3.5, DataSpell 2023.2.7,	https://w tbrains.co vacy- security/i fixed/	m/pri	A-JET-IN' 200624/	
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6 6-7	7 7-8	8-9	9-10

^{*} stands for all versions

			2023.2.7, 2023.3.7, 2024.1.3, 2024.2		
			EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
Affected Versi	ion(s): From (i	ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.3	
Insufficient ly Protected Credentials	10-Jun-2024 Scale 0-1	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.3.5,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-INTE- 200624/420

	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7 GitHub				2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-		
Insufficient ly Protected Credentials Credentials CVSSv3 Scoring Scale Tosum 2024 Tosum	Affected Vers	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.7	1
	ly Protected	10-Jun-2024	7.5	token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua	tbrains.com/pri vacy- security/issues-	
			1-2 2	-3 3-4 4-5	5-6 6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
weakness	Publish Date	CVSSV3	2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2023.2.4, 2023.3.5, 2024.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4	Patch	NCIIPC ID
			CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2023.3.0 Up to (exclu	ding) 2023.3.7	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-INTE- 200624/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			IDEA 2023.1.7,				
			2023.2.7, 2023.3.7,				
			2024.1.3, 2024.2				
			EAP3; Aqua				
			2024.1.2; CLion				
			2023.1.7, 2023.2.4,				
			2023.3.5, 2024.1.3,				
			2024.2 EAP2;				
			DataGrip 2023.1.3,				
			2023.2.4, 2023.3.5,				
			2024.1.4; DataSpell				
			2023.1.6, 2023.2.7,				
			2023.3.6, 2024.1.2,				
			2024.2 EAP1;				
			GoLand 2023.1.6,				
			2023.2.7, 2023.3.7,				
			2024.1.3, 2024.2				
			EAP3; MPS				
			2023.2.1, 2023.3.1,				
			2024.1 EAP2;				
			PhpStorm 2023.1.6,				
			2023.2.6, 2023.3.7,				
			2024.1.3, 2024.2				
			EAP3; PyCharm				
			2023.1.6, 2023.2.7,				
			2023.3.6, 2024.1.3,				
			2024.2 EAP2; Rider				
			2023.1.7, 2023.2.5,				
			2023.3.6, 2024.1.3;				
			RubyMine				
			2023.1.7, 2023.2.7,				
			2023.3.7, 2024.1.3,				
			2024.2 EAP4;				
			RustRover				
			2024.1.1;				
			WebStorm				
			2023.1.6, 2023.2.7,				
			2023.3.7, 2024.1.4				
			CVE ID: CVE-				
			2024-37051				
Product: mj	Product: mps						
Affected Ver	Affected Version(s): * Up to (excluding) 2023.2.1						

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; RyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.5, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-MPS- 200624/423

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Ver	sion(s): 2023.3	0	2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-MPS- 200624/424

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ph	pstorm		2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
		ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.3	
Insufficient ly Protected Credentials	Scale 0-1	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.3.5, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.4; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.2 EAP3	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PHPS-200624/425

		CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
Affected Ver	sion(s): * Up to	(excluding	g) 2023.1.6	I	I
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2;	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PHPS- 200624/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4		
Affected Ver	sion(s): From (i	ncluding)	CVE ID: CVE- 2024-37051 2023.3.0 Up to (exclu	ding) 2023.3.7	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PHPS- 200624/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051		
Affected Vers	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.6	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.3.5,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PHPS- 200624/428

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIF	PC ID
			2024.1.4; 2023.3.6, 2024.2 GoLand 2023.2.7, 2024.1.3, EAP3; 2023.2.1, 2024.1 PhpStorm 2023.2.6, 2024.1.3, EAP3; 2023.1.6, 2024.2 EA 2023.1.7, 2023.3.6, RubyMine 2023.1.7, 2023.3.7, 2024.2 RustRover 2024.1.1; WebStorm 2023.3.7, 2024.2 RustRover 2024.1.1; WebStorm 2023.3.7, 2024.2 RustRover 2024.1.1; WebStorm 2023.3.7, 2024.2 RustRover 2024.1.3, EAP3; 2023.3.7, 2024.2 RustRover 2024.1.1; WebStorm 2023.3.7, 2024.2 RustRover 2024.1.3,	DataSpell 2023.2.7, 2024.1.2, EAP1; 2023.3.6, 2024.2 MPS 2023.3.1, EAP2; 2023.3.7, 2024.2 PyCharm 2023.2.7, 2024.1.3, P2; Rider 2023.2.5, 2024.1.3; EAP4; 1 2023.2.7, 2024.1.3					
Product: py	charm								
Affected Ver	sion(s): From (i	including	2024.1.0 U	p to (excl	uding)	2024.1.	3		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	exposed party s JetBrains I version 20 less than	ites in DEs after 023.1 and : Intelli 2023.1.7	https tbrai vacy secu fixed	rity/issı	/pri	A-JET-P\ 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakiless	rubiisii Date	CV33V3	2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4	Pateri	NCIIPC ID
			CVE ID: CVE- 2024-37051		
Affected Vers	sion(s): * Up to	(excluding	g) 2023.1.6		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PYCH- 200624/430
CVSSv3 Scoring		1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			less than: IntelliJ					
			IDEA 2023.1.7,					
			2023.2.7, 2023.3.7,					
			2024.1.3, 2024.2					
			EAP3; Aqua					
			2024.1.2; CLion					
			2023.1.7, 2023.2.4,					
			2023.3.5, 2024.1.3,					
			2024.2 EAP2;					
			DataGrip 2023.1.3,					
			2023.2.4, 2023.3.5,					
			2024.1.4; DataSpell					
			2023.1.6, 2023.2.7,					
			2023.3.6, 2024.1.2,					
			2024.2 EAP1;					
			GoLand 2023.1.6,					
			2023.2.7, 2023.3.7,					
			2024.1.3, 2024.2					
			EAP3; MPS					
			2023.2.1, 2023.3.1,					
			2024.1 EAP2;					
			PhpStorm 2023.1.6,					
			2023.2.6, 2023.3.7,					
			2024.1.3, 2024.2					
			EAP3; PyCharm					
			2023.1.6, 2023.2.7,					
			2023.3.6, 2024.1.3,					
			2024.2 EAP2; Rider					
			2023.1.7, 2023.2.5,					
			2023.3.6, 2024.1.3;					
			RubyMine					
			2023.1.7, 2023.2.7,					
			2023.3.7, 2024.1.3,					
			2024.2 EAP4;					
			RustRover					
			2024.1.1;					
			WebStorm					
			2023.1.6, 2023.2.7,					
			2023.3.7, 2024.1.4					
			CVE ID: CVE-					
			2024-37051					
Affected Ver	ffected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7							

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.5, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PYCH-200624/431

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Ver	rsion(s): From (i	ncluding)	2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051 2023.3.0 Up to (exclu	ding) 2023.3.6	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-PYCH- 200624/432

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rie	lar		2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
	rsion(s): * Up to	(excluding	g) 2023.1.7		
Insufficient ly Protected Credentials	Scale 0-1	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RIDE- 200624/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4		
			CVE ID: CVE- 2024-37051		
Affected Vers	sion(s): From (i	ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.3	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2;	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RIDE- 200624/434
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4		
Affected Ver	 sion(s): From (i	ncluding)	CVE ID: CVE- 2024-37051 2023.3.0 Up to (exclu	ding) 2023.3.6	
Insufficient ly Protected Credentials	10-Jun-2024 Scale 0-1	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RIDE- 200624/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051		
Affected Vers	sion(s): From (i	ncluding)	2023.2.0 Up to (exclu	ding) 2023.2.5	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.2.4, 2023.3.5,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RIDE- 200624/436

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE I	D Patch	NCIIPC ID
			2024.1.4; DataSpe 2023.1.6, 2023.2. EAP GoLand 2023.1. 2023.2.7, 2023.3. 2024.1.3, 2024 EAP3; MF 2023.2.1, 2023.2.1, 2023.2.6, 2023.3. 2024.1.3, 2024.1.3, 2024.1.3, 2024.1.3, 2024.1.3, 2024.1.3, 2024.1.4, 2024.2 EAP2; Ride 2023.1.6, 2023.2. 2023.3.6, 2024.1. RubyMine 2023.1.7, 2023.2. 2023.3.7, 2024.1. RubyMine 2023.1.7, 2023.2. 2023.3.7, 2024.1. 2024.2 EAP RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2. 2023.3.7, 2024.1.4 CVE ID: CVE 2024-37051	Ill 7, 2, 1; 6, 7, 2 es 1, 2; 66, 7, 2 m 7, 3, er 5, 3; 7, 3, 4;	
Product: ru	hvmine				
	sion(s): * Up to	(excludin	g) 2023.1.7		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub acce token could be exposed to thire	https://ww tbrains.com vacy- iJ security/iss fixed/	A-JET-RUBY-
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7	7-8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID 2024.1.2; CLion 2023.1.7, 2023.2.4, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.2.7, 2023.3.7	Patch	NCIIPC ID
			CVE ID: CVE- 2024-37051		
Affected Vers	sion(s): From (i	ncluding)	2024.1.0 Up to (exclu	ding) 2024.1.3	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RUBY- 200624/438
CVSSv3 Scoring		1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			less than: IntelliJ					
			IDEA 2023.1.7,					
			2023.2.7, 2023.3.7,					
			2024.1.3, 2024.2					
			EAP3; Aqua					
			2024.1.2; CLion					
			2023.1.7, 2023.2.4,					
			2023.3.5, 2024.1.3,					
			2024.2 EAP2;					
			DataGrip 2023.1.3,					
			2023.2.4, 2023.3.5,					
			2024.1.4; DataSpell					
			2023.1.6, 2023.2.7,					
			2023.3.6, 2024.1.2,					
			2024.2 EAP1;					
			GoLand 2023.1.6,					
			2023.2.7, 2023.3.7,					
			2024.1.3, 2024.2					
			EAP3; MPS					
			2023.2.1, 2023.3.1,					
			2024.1 EAP2;					
			PhpStorm 2023.1.6,					
			2023.2.6, 2023.3.7,					
			2024.1.3, 2024.2					
			EAP3; PyCharm					
			2023.1.6, 2023.2.7,					
			2023.3.6, 2024.1.3,					
			2024.2 EAP2; Rider					
			2023.1.7, 2023.2.5,					
			2023.3.6, 2024.1.3;					
			RubyMine					
			2023.1.7, 2023.2.7,					
			2023.3.7, 2024.1.3,					
			2024.2 EAP4;					
			RustRover					
			2024.1.1;					
			WebStorm					
			2023.1.6, 2023.2.7,					
			2023.3.7, 2024.1.4					
			CVE ID: CVE-					
			2024-37051					
Affected Ver	Affected Version(s): From (including) 2023.2.0 Up to (excluding) 2023.2.7							

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; RyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RUBY- 200624/439

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 Ver	sion(s): From (i	ncluding)	2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051 2023.3.0 Up to (exclu	ding) 2023.3.7	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.6, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP3; RyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RUBY- 200624/440

1-2

3-4

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ru	ctrovor		2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE- 2024-37051		
	sion(s): * Up to	(excludin	g) 2024.1.1		
Insufficient ly Protected Credentials	3 Scale 0-1	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7,	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-RUST- 200624/441

	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2024.1.0 Up to (excluding) 2024.1.4 GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS				2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-		
CitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS A-JET-WEBS-200624/442	Product: we	ebstorm				
token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS	Affected Ver	sion(s): From (i	ncluding)		iding) 2024.1.4	
	ly Protected	10-Jun-2024	7.5	token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS	https://www.je tbrains.com/pri vacy- security/issues-	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-		
Affected Ver	sion(s): * Up to	(excluding	2024-37051 g) 2023.1.6		
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1;	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-WEBS- 200624/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4 CVE ID: CVE-2024-37051		
Affected Ver	sion(s): From (i	ncluding)	2023.3.0 Up to (exclu	ding) 2023.3.7	
Insufficient ly Protected Credentials	10-Jun-2024	7.5	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2024.1.3, 2024.2 EAP3; Aqua	https://www.je tbrains.com/pri vacy- security/issues- fixed/	A-JET-WEBS- 200624/445

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	C ID
Weakness	Publish Date	CVSSv3	Description of 2024.1.2; 2023.1.7, 2 2024.2 DataGrip 2 2023.2.4, 2 2024.1.4; D 2023.1.6, 2 2024.2 GoLand 2 2023.2.7, 2 2024.1 PhpStorm 2 2023.2.6, 2 2024.1.3, EAP3; 2023.2.6, 2 2024.1.3, EAP3; 2023.2.6, 2 2024.1.3, EAP3; 2023.2.6, 2 2024.1.3, EAP3; 2023.1.6, 2 2023.3.6, 2 2024.2 EAP 2023.1.7, 2 2023.3.6, 2 RubyMine 2023.1.7, 2 2023.3.7, 2 2024.2 RustRover 2024.1.1; WebStorm 2023.1.6, 2	CLion (023.2.4, 024.1.3, EAP2; 023.3.5, 024.1.2, EAP1; 023.3.7, 2024.2 MPS (023.3.7, 2024.2 CYCharm (023.2.7, 024.1.3, 2; Rider (023.2.5, 024.1.3; 024.1.3, EAP4; 023.2.7, 024.1.3;		Patch		NCIIP	CID
			2023.3.7, 20 CVE ID: 2024-3705	CVE-					
Vendor: kate	ello_project				<u> </u>				
Product: kat	ello								
Affected Vers	ion(s): -								
Improper Neutralizat ion of Input	05-Jun-2024	4.8	A flaw was the Katello	plugin	N/A			A-KAT-K 200624/	
CVSSv3 Scoring S	Scale 0-1	1-2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
stands for all ver			Page 264 o						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			it is possible to store malicious JavaScript code in the "Description" field of a user. This code can be executed when opening certain pages, for example, Host Collections. CVE ID: CVE-		
Vendor: la-s	studioweb		2024-4812		
	ement_kit_for_c	elemento	r		
Affected Ver	sion(s): * Up to	(excluding	g) 1.3.7.4		
Missing Authorizati on	10-Jun-2024	8.8	Missing Authorization vulnerability in LA- Studio LA-Studio Element Kit for Elementor.This issue affects LA- Studio Element Kit for Elementor: from n/a through 1.3.6. CVE ID: CVE- 2024-35725	N/A	A-LAELEM- 200624/447
Vendor: lan	gflow				
Product: lar					
Affected Ver	sion(s): * Up to	(including			
N/A	10-Jun-2024	9.8	Langflow through 0.6.19 allows remote code execution if untrusted users are able to reach the "POST /api/v1/custom_component" endpoint	N/A	A-LAN-LANG- 200624/448

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
Vendor: lift	erlms		and provide a Python script. CVE ID: CVE-2024-37014								
Affected Ver	Affected Version(s): * Up to (excluding) 7.6.3										
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	05-Jun-2024	6.5	The LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to SQL Injection via the orderBy attribute of the lifterIms_favorites shortcode in all versions up to, and including, 7.6.2 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 Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 95706%40lifter lms%2Ftrunk& old=3094820% 40lifterlms%2F trunk&sfp_emai l=&sfph_mail=	A-LIF-LIFT- 200624/449						

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE	ID	Patch		NCIIPC ID		
				/E-					
Vandam lun	O.W.Y.		2024-4743						
Vendor: lun									
Product: lui									
Affected Ver	sion(s): 1.2.13								
N/A	09-Jun-2024	8.1	datasets not own by the organization. To issue arises due the application properly validate the ownership dataset promand their variation against organization project of requesting users a resunauthorized modifications dataset promican occur, leading to altered removed dataset prompts with proper authorization. To vulnerability impacts	of rol to get, npt for led eir his to not ing of pts ons che As ult, to pts ing or set out	1		A-LUN-LU 200624/4		
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6	6-7	7-8	8-9	9-10	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
			information, potentially affecting the results of experiments. CVE ID: CVE- 2024-5389								
Vendor: lylr	ne										
Product: lylme_spage											
Affected Ver	sion(s): 1.9.5										
Server- Side Request Forgery (SSRF)	04-Jun-2024	9.1	LyLme_spage v1.9.5 is vulnerable to Server-Side Request Forgery (SSRF) via the get_head function. CVE ID: CVE- 2024-36675	N/A	A-LYL-LYLM- 200624/451						
Vendor: ma	ster-addons										
Product: ma	aster_addons										
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.6.2								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	6.1	The Master Addons - Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Navigation Menu widget of the plugin's Mega Menu extension in all versions up to, and including, 2.0.6.1 due to insufficient input sanitization and output escaping on	https://plugins. trac.wordpress. org/changeset/ 3096299/maste r-addons	A-MAS-MAST- 200624/452						

	CVSSv3 Scoring Scale
×	* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-5542		
Missing Authorizati on	07-Jun-2024	5.3	The Master Addons - Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ma- template' REST API route in all versions up to, and including, 2.0.6.1. This makes it possible for unauthenticated attackers to create or modify existing Master Addons templates or make settings modifications related to these templates.	https://plugins. trac.wordpress. org/changeset/ 3096299/maste r-addons	A-MAS-MAST- 200624/453

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-5382		
Vendor: me	lapress				
Product: me	elapress_login_	security			
Affected Ver	sion(s): * Up to	(excluding	g) 1.3.1		
Inclusion of Functionali ty from Untrusted Control Sphere	10-Jun-2024	7.2	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Melapress MelaPress Login Security allows PHP Remote File Inclusion.This issue affects MelaPress Login Security: from n/a through 1.3.0. CVE ID: CVE-2024-35650	N/A	A-MEL-MELA- 200624/454
Vendor: me	owapps				
Product: da	tabase_cleane	ŗ			
Affected Ver	sion(s): * Up to	(excluding	g) 1.0.6		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	4.9	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Jordy Meow Database Cleaner allows Relative Path Traversal.This issue affects Database Cleaner:	N/A	A-MEO-DATA- 200624/455

ı	CVSSV3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	/-8	8-9	9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			from n/a through 1.0.5.			
			CVE ID: CVE- 2024-35712			
Vendor: me	tagauss					
Product: ev	entprime					
Affected Ver	sion(s): * Up to	(excluding	g) 3.3.5			
Missing Authorizati on	09-Jun-2024	9.8	Missing Authorization vulnerability in Metagauss EventPrime.This issue affects EventPrime: from n/a through 3.3.4.	N/A	A-MET-EVEN- 200624/456	
			CVE ID: CVE- 2024-31275			
Product: pr	ofilegrid					
Affected Ver	sion(s): * Up to	(excluding	g) 5.8.7			
Missing Authorizati on	05-Jun-2024	4.3	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pm_dismissible_not ice and pm_wizard_update _group_icon functions in all versions up to, and including, 5.8.6. This makes it possible for authenticated	https://plugins. trac.wordpress. org/changeset/ 3095503/profil egrid-user- profiles-groups- and- communities/tr unk/admin/clas s-profile-magic- admin.php?cont extall=1	A-MET-PROF- 200624/457	
			authenticated			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers, with Subscriber-level access and above, to change arbitrary options to the value '1' or change group icons. CVE ID: CVE-2024-5453		
Vendor: mi	ntplexlabs				
Product: an	<u>. </u>				
Affected Ver	sion(s): * Up to	(including	g) 1.5.4		
Server- Side Request Forgery (SSRF)	05-Jun-2024	7.5	Request Forgery (SSRF) vulnerability exists in the latest version of mintplex-labs/anything-llm, allowing attackers to bypass the official fix intended to restrict access to intranet IP addresses and protocols. Despite efforts to filter out intranet IP addresses starting with 192, 172, 10, and 127 through regular expressions and limit access protocols to HTTP and HTTPS, attackers can still bypass these restrictions using alternative representations of IP addresses and accessing other	N/A	A-MIN-ANYT- 200624/458

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Mo			ports running on localhost. This vulnerability enables attackers to access any asset on the internal network, attack web services on the internal network, scan hosts on the internal network, and potentially access AWS metadata endpoints. The vulnerability is due to insufficient validation of usersupplied URLs, which can be exploited to perform SSRF attacks. CVE ID: CVE-2024-4084		
Product: py	mongo				
	sion(s): * Up to	(excluding	g) 4.6.3		
Out-of- bounds Read	-of- nds 05-Jun-2024 8.1		An out-of-bounds read in the 'bson' module of PyMongo 4.6.2 or earlier allows deserialization of malformed BSON provided by a Server to raise an exception which may contain arbitrary application memory.	https://jira.mo ngodb.org/bro wse/PYTHON- 4305	A-MON-PYMO- 200624/459
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-	8 8-9 9-10
* stands for all ve					

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	C ID		
			CVE ID: 2024-562	CVE-							
Vendor: mo	veaddons										
Product: mo	ove_addons_fo	r_elemen	tor								
Affected Ver	sion(s): * Up to	(excludin	g) 1.3.0								
Missing Authorizati on	04-Jun-2024	7.3	Missing Authorizat vulnerabili moveaddo Addons Elementor issue affec Addons Elementor n/a throug CVE ID: 2024-305	ty in ns Move for This ets Move for for from h 1.2.9.	N/A			A-MOV-N 200624/			
Vendor: multivendorx											
Product: mu	ıltivendorx										
Affected Ver	sion(s): * Up to	(excludin	g) 4.1.12								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	Scripting 'hover_aning parameter versions un including, due to institute to institute the same and escaping.	ce – herce or ce lugin for s is to ross-Site via the mation' in all p to, and 4.1.11 sufficient nitization output This	trac.v	://plug wordpre changes 002/	ess.	A-MUL-M 200624/			
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-5259		
Affected Ver	sion(s): * Up to	(excluding	g) 4.1.4		
Missing Authorizati on	09-Jun-2024	8.8	Missing Authorization vulnerability in MultiVendorX WC Marketplace.This issue affects WC Marketplace: from n/a through 4.1.3. CVE ID: CVE- 2024-31304	N/A	A-MUL-MULT- 200624/462
Vendor: net	gsm				
Product: ne	tgsm				
Affected Ver	sion(s): * Up to	(including	g) 2.9.16		
Missing Authorizati on	04-Jun-2024	9.8	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16. CVE ID: CVE-	N/A	A-NET-NETG- 200624/463
Missing Authorizati on	10-Jun-2024	6.3	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16.	N/A	A-NET-NETG- 200624/464

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID: CVE- 2024-4746				
Vendor: netty							
Product: ne	tty-incubator-	codec-oh	ttp				
Affected Ver	sion(s): From (i	ncluding)	0.0.3 Up to (excluding	g) 0.0.11			
Integer Overflow or Wraparoun d	04-Jun-2024	9.1	netty-incubator- codec-ohttp is the OHTTP implementation for netty. BoringSSLAEADCo ntext keeps track of how many OHTTP responses have been sent and uses this sequence number to calculate the appropriate nonce to use with the encryption algorithm. Unfortunately, two separate errors combine which would allow an attacker to cause the sequence number to overflow and thus the nonce to repeat. CVE ID: CVE-2024-36121	https://github.c om/netty/netty -incubator- codec- ohttp/security/ advisories/GHS A-g762-h86w- 8749	A-NET-NETT- 200624/465		
Vendor: online_discussion_forum_project							
Product: online_discussion_forum							
Affected Ver	Sion(S): 1.0		A vulnorability was				
Improper Neutralizat ion of Special Elements used in an	07-Jun-2024	9.8	A vulnerability was found in itsourcecode Online Discussion Forum 1.0. It has been rated as	N/A	A-ONL-ONLI- 200624/466		
CVSSv3 Scoring	Scale 0-1	1-2 2	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')			critical. This issue affects some unknown processing of the file register_me.php. The manipulation of the argument eaddress 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-267407. CVE ID: CVE-2024-5733		
Unrestricte d Upload of File with Dangerous Type	07-Jun-2024	8.8	A vulnerability classified as critical has been found in itsourcecode Online Discussion Forum 1.0. Affected is an unknown function of the file /members/poster. php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be	N/A	A-ONL-ONLI- 200624/467

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			used. The identifier of this vulnerability is VDB-267408. CVE ID: CVE-2024-5734			
Vendor: ope	entelemetry					
Product: co	nfiggrpc					
Affected Vers	sion(s): * Up to	(excluding	g) 0.102.1			
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Jun-2024	7.5	The OpenTelemetry Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1. CVE ID: CVE-2024-36129	https://github.c om/open- telemetry/open telemetry- collector/pull/1 0289, https://github.c om/open- telemetry/open telemetry- collector/pull/1 0323, https://opentel emetry.io/blog/ 2024/cve-2024- 36129	A-OPE-CONF- 200624/468	
Product: confighttp						
Affected Vers	sion(s): * Up to	(excluding	g) 0.102.0			
Improper Restriction	05-Jun-2024	7.5	The OpenTelemetry	https://github.c om/open-	A-OPE-CONF- 200624/469	

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1. CVE ID: CVE-2024-36129	telemetry/open telemetry- collector/pull/1 0289, https://github.c om/open- telemetry/open telemetry- collector/pull/1 0323, https://opentel emetry.io/blog/ 2024/cve-2024- 36129	
Product: op	entelemetry_c	ollector			
Affected Vers	sion(s): * Up to	(excluding	g) 0.102.1		
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Jun-2024	7.5	The OpenTelemetry Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash	https://github.c om/open- telemetry/open telemetry- collector/pull/1 0289, https://github.c om/open- telemetry/open telemetry- collector/pull/1 0323, https://opentel emetry.io/blog/	A-OPE-OPEN- 200624/470

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1. CVE ID: CVE-2024-36129	2024/cve-2024- 36129	
Vendor: opr	nc				
Product: wo	ocommerce_d	ropshipp	ing		
Affected Vers	sion(s): * Up to	(including	g) 5.0.4		
Missing Authorizati on	09-Jun-2024	5.3	Missing Authorization vulnerability in OPMC WooCommerce Dropshipping.This issue affects WooCommerce Dropshipping: from n/a through 5.0.4. CVE ID: CVE- 2024-35748	N/A	A-OPM-WOOC- 200624/471
Vendor: ore	tnom23			l	
Product: on	line_medicine ₋	ordering	system		_
Affected Vers	sion(s): 1.0				
N/A	10-Jun-2024	9.1	Sourcecodester Online Medicine Ordering System 1.0 is vulnerable to Arbitrary file deletion vulnerability as the backend settings	N/A	A-ORE-ONLI- 200624/472
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have the function of deleting pictures to delete any files.		
			CVE ID: CVE- 2024-32167		
Vendor: ovi	c_importer_pr	oject			
Product: ov	ic_importer				
Affected Ver	sion(s): * Up to	(including	g) 1.6.3		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ovic Team Ovic Importer allows Path Traversal.This issue affects Ovic Importer: from n/a through 1.6.3. CVE ID: CVE- 2024-35754	N/A	A-0VI-0VIC- 200624/473
Vendor: par	risneo				
	lms_web_ui				
Affected Ver	sion(s): 9.6				
Cross-Site Request Forgery (CSRF)	10-Jun-2024	8.1	A Cross-Site Request Forgery (CSRF) vulnerability exists in the clear_personality_fi les_list function of the parisneo/lollms- webui v9.6. The vulnerability arises from the use of a GET request to clear personality	N/A	A-PAR-LOLL- 200624/474

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files list, which lacks proper CSRF protection. This flaw allows attackers to trick users into performing actions without their consent, such as deleting important files on the system. The issue is present in the application's handling of requests, making it susceptible to CSRF attacks that could lead to unauthorized actions being performed on behalf of the user. CVE ID: CVE-2024-4328		
Vendor: pdf	crowd				
Product: sav	ve_as_pdf_plug	in			
Affected Vers	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This issue affects Save as PDF plugin by Pdfcrowd: from n/a through 3.2.3.	N/A	A-PDF-SAVE- 200624/475
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7	7-8 8-9 9-10
* stands for all ve			Page 282 of 471		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-35649		
Vendor: pha	rmacy\/medi	cal_store	_point_of_sale_system	n_project	
Product: ph	armacy\/med	ical_store	e_point_of_sale_syste	m	
Affected Vers	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	07-Jun-2024	9.8	Sourcecodester Pharmacy/Medical Store Point of Sale System 1.0 is vulnerable SQL Injection via login.php. This vulnerability stems from inadequate validation of user inputs for the email and password parameters, allowing attackers to inject malicious SQL queries. CVE ID: CVE- 2024-36673	N/A	A-PHA-PHAR- 200624/476
Vendor: PH	P				
Product: ph	p				
Affected Vers	sion(s): From (i	ncluding)	5.0.0 Up to (excluding	g) 8.1.29	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	09-Jun-2024 Scale 0-1	9.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line	N/A	A-PHP-PHP- 200624/477

CVSSv3 Scoring Scale 0-1
* stands for all versions

given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. CVE ID: CVE-2024-4577 Affected Version(s): From (including) 7.3.27 Up to (including) 7.3.33 In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL) IDATE_URL) for certain types of URLs in function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.	Weakness	Publish Date	CVSSv3	Description	n & CVE ID		Patch		NCII	PC ID
Insufficient Verification of Data Authenticit y 1.				functions. module misinterp characters options, w allow a user to pas to PHP bir run, and th the sourc scripts, arbitrary on the ser CVE ID:	PHP CGI may ret those s as PHP which may malicious ss options hary being hus reveal e code of run PHP code ver, etc.					
Unsufficient Verification n of Data Authenticit y 5.3 O9-Jun-2024 Unsufficient Verification n of Data Authenticit y 1.3 O9-Jun-2024 O9-Jun-202	Affected Vers	sion(s): From (i	ncluding)	7.3.27 Up t	o (includi	ng) 7.3	3.33			
	Verificatio n of Data Authenticit	09-Jun-2024	5.3	versions 8 before 8.2 before 8.3 a code lo filtering such as when URLs (FIL IDATE_UR certain URLs the will result user inf (username password URLs) treated user inf This may l downstrea accepting URLs as parsing	3.1.* 1.29, 8.2.* 2.20, 8.3.* 3.8, due to gic error, functions filter_var validating TER_VAL 3.1 for types of function in invalid formation e + part of being as valid formation. ead to the am code invalid valid and them	http: om/ src/s visor w8q r27v	php/phpsecurity, ries/GHS r-v226-	o- /ad		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-5458		
Affected Ver	sion(s): From (i	ncluding)	7.4.15 Up to (includin	ig) 7.4.33	
Insufficient Verificatio n of Data Authenticit y	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL IDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. CVE ID: CVE-2024-5458	https://github.c om/php/php- src/security/ad visories/GHSA- w8qr-v226- r27w	A-PHP-PHP- 200624/479
Affected Ver	sion(s): From (i	ncluding)	8.0.2 Up to (including	3) 8.0.30	I
Insufficient Verificatio n of Data Authenticit y	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL	https://github.c om/php/php- src/security/ad visories/GHSA- w8qr-v226- r27w	A-PHP-PHP- 200624/480

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. CVE ID: CVE-2024-5458		
Affected Ver	 <mark>sion(s): From (i</mark>	ncluding)	8.1.0 Up to (excluding	g) 8.1.29	
Improper Encoding or Escaping of Output	09-Jun-2024 Scale 0-1	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary	N/A	A-PHP-PHP- 200624/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands in Windows shell. CVE ID: CVE-2024-5585		
Observable Discrepanc y	09-Jun-2024	5.9	The openssl_private_de crypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_ PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable.	N/A	A-PHP-PHP- 200624/482
* stands for all ve		1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PHP Windows builds for the versions 8.1.29, 8.2 .20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability. CVE ID: CVE-2024-2408		
Insufficient Verificatio n of Data Authenticit y	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL IDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. CVE ID: CVE-2024-5458	https://github.c om/php/php- src/security/ad visories/GHSA- w8qr-v226- r27w	A-PHP-PHP- 200624/483
Affected Vers	sion(s): From (i	ncluding)	8.2.0 Up to (excluding	g) 8.2.20	
Improper Neutralizat ion of	09-Jun-2024	9.8	In PHP versions 8.1.* before 8.1.29, 8.2.*	N/A	A-PHP-PHP- 200624/484
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 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 OS Command ('OS Command Injection')			before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. CVE ID: CVE-2024-4577		
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient	N/A	A-PHP-PHP- 200624/485

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. CVE ID: CVE-2024-5585		
Observable Discrepanc y	09-Jun-2024	5.9	The openssl_private_de crypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_ PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for	N/A	A-PHP-PHP- 200624/486

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable.		
			PHP Windows builds for the versions 8.1.29, 8.2 .20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability. CVE ID: CVE-		
Insufficient Verificatio n of Data Authenticit y	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL IDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and	https://github.c om/php/php- src/security/ad visories/GHSA- w8qr-v226- r27w	A-PHP-PHP- 200624/487

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (i	ncluding)	parsing them incorrectly. CVE ID: CVE-2024-5458 8.3.0 Up to (excluding	g) 8.3.8	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	09-Jun-2024	9.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc. CVE ID: CVE-2024-4577	N/A	A-PHP-PHP- 200624/488
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874	N/A	A-PHP-PHP- 200624/489

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. CVE ID: CVE-2024-5585		
Observable Discrepanc y	09-Jun-2024	5.9	The openssl_private_de crypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_ PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These	N/A	A-PHP-PHP- 200624/490

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable. PHP Windows builds for the versions 8.1.29, 8.2 .20 and 8.3.8 and above include	
OpenSSL patches that fix the vulnerability. CVE ID: CVE-2024-2408	
$\begin{bmatrix} 1 & 0 \end{bmatrix}$ $\begin{bmatrix} 0 \end{bmatrix}$	A-PHP-PHP- 200624/491

^{*} stands for all versions

Weakness	Publish Date	CVSSv	3 De	scription	& CVE ID		Patch		NC	IIPC ID
			pas UR tre use Th do acc UR par	(username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.						
				E ID: 24-5458	CVE B	-				
Vendor: Pin	ncore									
Product: pir	ncore									
Affected Ver	sion(s): From (includin	ng) 11.0	0.0 Up to	(exclud	ling) 1	1.2.4			
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.5	Sou Exj Ma Pla Pir gen use ser file the sca rec thu att cre mu siz ori vul fixe	perience nageme atform. ncore the neration ed to flever with es. By the file extending fact quested ambnail, ackers that files	nt The numbnaican be lood the large changing ension of the car of the Thi ty i 2.4. CVE	httt om e e g g htt om g ht	ps://gith a/pimcore ore/secu dvisories/ -277c-5vv	e/pi mit/ 0f1 4e2 a06 ub.c e/pi mit/ 380 82e 4bd ub.c e/pi rity	A-PIM- 20062	_
Vendor: por	rty									
Product: po	werbank									
CVSSv3 Scoring	Scale 0-1	1-2	2-3	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 Ver	sion(s): * Up to	(excluding	g) 2.02	L	L
N/A	05-Jun-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PORTY Smart Tech Technology Joint Stock Company PowerBank Application allows Retrieve Embedded Sensitive Data.This issue affects PowerBank Application: before 2.02. CVE ID: CVE-2024-1662	N/A	A-POR-POWE- 200624/493
Vendor: pq-	crystals				
Product: ky	ber				
Affected Ver	sion(s): * Up to	(excluding	g) 2024-06-03		
Observable Discrepanc y	10-Jun-2024	7.5	The Kyber reference implementation before 9b8d306, when compiled by LLVM Clang through 18.x with some common optimization options, has a timing side channel that allows attackers to recover an ML-KEM 512 secret key in minutes. This occurs because poly_frommsg in poly.c does not prevent Clang from	https://github.c om/pq- crystals/kyber/ commit/9b8d3 0698a3e7449ae b34e62339d41 76f11e3c6c	A-PQKYBE- 200624/494

Accessible to External Parties O5-Jun-2024 9,8 I read/write any files in the directory and subdirectories of where the victim runs interactsh-server via anonymous login. CVE ID: CVE-2024-5262 Vendor: purechat Affected Version(s): * Up to (excluding) 2.3 Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat. This issue affects Pure Chat: from n/a through 2.22. A-PUR-PURE 200624/496	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 0.0.6 Up to (excluding) 1.2.0 Files or Directories Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactsh-server via anonymous login. CVE ID: CVE-2024-5262 Vendor: pure_chat Affected Version(s): * Up to (excluding) 2.3 Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat. This issue affects Pure Chat: from n/a through 2.22.				vulnerable secret- dependent branch. CVE ID: CVE-		
Affected Version(s): From (including) 0.0.6 Up to (excluding) 1.2.0 Files or Directories Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactsh server via anonymous login. CVE ID: CVE-2024-5262 Vendor: pure_chat A-PRO-INTE 200624/495 A-PRO-INTE 200624/495	Vendor: pro	jectdiscovery				
Files or Directories Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactsh server via anonymous login. CVE ID: CVE 2024-5262 Vendor: purechat Product: pure_chat Affected Version(s): * Up to (excluding) 2.3 Cross-Site Request Forgery (CSRF) O5-Jun-2024 4.3 Files or Directories Accessible to External Parties https://github.c om/projectdisc owery/interacts h/pull/874 A-PRO-INTE 200624/495 A-PUR-PURE 200624/496	Product: int	eractsh				
Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactsh server via anonymous login. CVE ID: CVE-2024-5262 Vendor: purechat Product: pure_chat Affected Version(s): * Up to (excluding) 2.3 Cross-Site Request Forgery (CSRF) Cross-Site Request Forgery (CSRF) CCRSF) A-PRO-INTE 200624/495 https://github.com/projectdisc om/projectdisc overy/interacts h/pull/874 A-PRO-INTE 200624/495	Affected Vers	sion(s): From (i	ncluding)	0.0.6 Up to (excluding	g) 1.2.0	
Product: pure_chat Affected Version(s): * Up to (excluding) 2.3 Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22. A-PUR-PURE 200624/496	Directories Accessible to External	05-Jun-2024	9.8	Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactshserver via anonymous login. CVE ID: CVE-	om/projectdisc overy/interacts	A-PRO-INTE- 200624/495
Affected Version(s): * Up to (excluding) 2.3 Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22. A-PUR-PURE 200624/496						
Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22. Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22.	-		() 1	222		
Cross-Site Request Forgery (CSRF) 05-Jun-2024 4.3 Forgery Chat by Ruby Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22. A-PUR-PURE 200624/496	Affected vers	sion(s): " Up to	excluain			
CVE ID: CVE- 2024-35673	Request Forgery	05-Jun-2024	4.3	Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22. CVE ID: CVE-	N/A	A-PUR-PURE- 200624/496

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Product: qi_	blocks									
Affected Version(s): * Up to (excluding) 1.3.0										
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	The Qi Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-5221	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 97241%40qi- blocks%2Ftrun k&old=3094374 %40qi- blocks%2Ftrun k&sfp_email=&s fph_mail=	A-QOD-QI_B- 200624/497					
Vendor: Red										
-	enshift_contain	ner_platfo	orm							
Affected Ver	sion(s): 4.0									
Authentica tion Bypass by Spoofing	05-Jun-2024	7.5	A flaw was found in OpenShift's Telemeter. If certain conditions are in place, an attacker can use a forged token to bypass the issue ("iss") check during JSON web token	https://access.r edhat.com/secu rity/cve/CVE- 2024-5037, https://bugzilla .redhat.com/sh ow_bug.cgi?id= 2272339, https://github.c om/kubernetes	A-RED-OPEN- 200624/498					
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10					

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(JWT) authentication. CVE ID: CVE- 2024-5037	/kubernetes/pu ll/123540	
Product: op	enshift_distrib	uted_tra	cing		
Affected Ver	sion(s): 2.0				
Authentica tion Bypass by Spoofing	05-Jun-2024	7.5	A flaw was found in OpenShift's Telemeter. If certain conditions are in place, an attacker can use a forged token to bypass the issue ("iss") check during JSON web token (JWT) authentication. CVE ID: CVE-2024-5037	https://access.r edhat.com/secu rity/cve/CVE- 2024-5037, https://bugzilla .redhat.com/sh ow_bug.cgi?id= 2272339, https://github.c om/kubernetes /kubernetes/pu ll/123540	A-RED-OPEN- 200624/499
Product: sa	tellite				
Affected Ver	sion(s): 6.0				
N/A	05-Jun-2024	6.2	A flaw was found in foreman-installer when puppet-candlepin is invoked cpdb with thepassword parameter. This issue leaks the password in the process list and allows an attacker to take advantage and obtain the password. CVE ID: CVE-2024-3716	N/A	A-RED-SATE- 200624/500
Improper Neutralizat	05-Jun-2024	4.8	A flaw was found in the Katello plugin	N/A	A-RED-SATE- 200624/501

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			for Foreman, where it is possible to store malicious JavaScript code in the "Description" field of a user. This code can be executed when opening certain pages, for example, Host Collections. CVE ID: CVE-2024-4812		
Vendor: rep	 outeinfosystem	IS			
Product: art					
Affected Ver	sion(s): * Up to	(excluding	g) 6.4.1		
Missing Authorizati on	09-Jun-2024	Missing Authoriza vulnerabi reputeinfo ARForms.		N/A	A-REP-ARFO- 200624/502
** 1	.1		2024-32705		
Vendor: rise					
	easy_builder sion(s): * Up to	(excluding	g) 2.1		
Missing Authorizati on	04-Jun-2024	8.8	Missing Authorization vulnerability in RT Easy Builder – Advanced addons for Elementor.This issue affects RT Easy Builder – Advanced addons for Elementor:	N/A	A-RIS-RT_E- 200624/503

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 n/a through 2.0.		
			CVE ID: CVE- 2024-30484		
Vendor: roy	al-elementor-	addons			
Product: ro	yal_elementor_	_addons			
Affected Ver	sion(s): * Up to	(excluding	g) 1.3.977		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-Jun-2024	5.4	The Royal Elementor Addons and Templates for WordPress is vulnerable to Stored Cross-Site Scripting via the 'inline_list' parameter in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4488	https://plugins. trac.wordpress. org/changeset/ 3097775/	A-ROY-ROYA- 200624/504
Improper Neutralizat ion of Input During Web Page Generation	07-Jun-2024	5.4	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to	https://plugins. trac.wordpress. org/changeset/ 3097775/	A-ROY-ROYA- 200624/505

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Stored Cross-Site Scripting via the 'custom_upload_mi mes' function in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4489		
Vendor: Ru	byonrails				
Product: ra	ils				
Affected Ver	sion(s): 7.2.0				
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is	https://github.c om/rails/rails/ commit/35858f 1d9d57f6c4050 a8d9ab754bd5 d088b4523, https://github.c om/rails/rails/ security/adviso ries/GHSA- fwhr-88qx-h9g7	A-RUB-RAIL- 200624/506

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. CVE ID: CVE-2024-28103		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	6.1	Action Text brings rich text content and editing to Rails. Instances of ActionText::Attach able::ContentAttach ment included within a rich_text_area tag could potentially contain unsanitized HTML. This vulnerability is fixed in 7.1.3.4 and 7.2.0.beta2. CVE ID: CVE-2024-32464	https://github.c om/rails/rails/ commit/e215bf 3360e6dfe1497 c1503a495e384 ed6b0995	A-RUB-RAIL- 200624/507
Affected Ver	sion(s): From (i	ncluding)	6.1.0 Up to (excluding	g) 6.1.7.8	I
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3.	https://github.c om/rails/rails/ commit/35858f 1d9d57f6c4050 a8d9ab754bd5 d088b4523, https://github.c om/rails/rails/ security/adviso ries/GHSA- fwhr-88qx-h9g7	A-RUB-RAIL- 200624/508
A CC - 1 1 1 7	-:(-) B:	-1-1:	2024-28103) 7 0 0 4	
Affected Vers	sion(s): From (i	ncluding)	7.0.0 Up to (excluding	g) /.0.8.4	

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. CVE ID: CVE-2024-28103	https://github.c om/rails/rails/ commit/35858f 1d9d57f6c4050 a8d9ab754bd5 d088b4523, https://github.c om/rails/rails/ security/adviso ries/GHSA- fwhr-88qx-h9g7	A-RUB-RAIL- 200624/509
Affected Ver	sion(s): From (i	ncluding)	7.1.0 Up to (excluding	g) 7.1.3.4	
N/A	04-Jun-2024	9.8	Action Pack is a framework for handling and responding to web requests. Since 6.1.0, the application configurable Permissions-Policy is only served on responses with an HTML related Content-Type. This vulnerability is fixed in 6.1.7.8, 7.0.8.2, and 7.1.3.3. CVE ID: CVE-2024-28103	https://github.c om/rails/rails/ commit/35858f 1d9d57f6c4050 a8d9ab754bd5 d088b4523, https://github.c om/rails/rails/ security/adviso ries/GHSA- fwhr-88qx-h9g7	A-RUB-RAIL- 200624/510
Improper Neutralizat ion of Input During Web Page	04-Jun-2024	6.1	Action Text brings rich text content and editing to Rails. Instances of ActionText::Attach	https://github.c om/rails/rails/ commit/e215bf 3360e6dfe1497	A-RUB-RAIL- 200624/511

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			able::ContentAttac hment included within a rich_text_area tag could potentially contain unsanitized HTML. This vulnerability is fixed in 7.1.3.4 and 7.2.0.beta2. CVE ID: CVE-2024-32464	c1503a495e384 ed6b0995	
Vendor: sale	esagility				
Product: sui	itecrm				
Affected Vers	sion(s): * Up to	(excludin	g) 7.14.4		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	9.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in events response entry point allows for a SQL injection attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36412	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-xjx2- 38hv-5hh8	A-SAL-SUIT- 200624/512
Improper Neutralizat ion of Input During Web Page Generation	10-Jun-2024	9	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-3www- 6rqc-rm7j	A-SAL-SUIT- 200624/513
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			and 8.6.1, an unverified IFrame can be added some some inputs, which could allow for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36417		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in the 'Alerts' controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36408	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-2g8f- gjrr-x5cg	A-SAL-SUIT- 200624/514
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024 Scale 0-1	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-pxq4- vw23-v73f	A-SAL-SUIT- 200624/515

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tree data entry point. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36409		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax messages count controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36410	N/A	A-SAL-SUIT- 200624/516
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024 Scale 0-1	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax displayView controller. Versions 7.14.4 and 8.6.1	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-9rvr- mcrf-p4p7	A-SAL-SUIT- 200624/517

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a fix for this issue. CVE ID: CVE-2024-36411		
Unrestricte d Upload of File with Dangerous Type	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in uploaded file verification in products allows for remote code execution. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36415	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-c82f- 58jv-jfrh	A-SAL-SUIT- 200624/518
N/A	10-Jun-2024	7.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a deprecated v4 API example with no log rotation allows denial of service by logging excessive data. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-jrpp- 22g3-2j77	A-SAL-SUIT- 200624/519

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-36416		
Weak Password Recovery Mechanism for Forgotten Password	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, a user password can be reset from an unauthenticated attacker. The attacker does not get access to the new password. But this can be annoying for the user. This attack is also dependent on some password reset functionalities being enabled. It also requires the system using php 7, which is not an officially supported version. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36407	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-6p2f- wwx9-952r	A-SAL-SUIT- 200624/520
Server- Side Request Forgery (SSRF)	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-wg74- 772c-8gr7	A-SAL-SUIT- 200624/521

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to versions 7.14.4 and 8.6.1, a vulnerability in the connectors file verification allows for a server-side request forgery attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36414		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the import module error view allows for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36413	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-ph2c- hvvf-r273	A-SAL-SUIT- 200624/522
Affected Vers	sion(s): From (i	ncluding)	8.0.0 Up to (excluding	g) 8.6.1	
Improper Neutralizat ion of Special Elements used in an SQL Command	10-Jun-2024	9.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-xjx2- 38hv-5hh8	A-SAL-SUIT- 200624/523

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			vulnerability in events response entry point allows for a SQL injection attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36412		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	9	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, an unverified IFrame can be added some some inputs, which could allow for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36417	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-3www- 6rqc-rm7j	A-SAL-SUIT- 200624/524
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024 Scale 0-1	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in the 'Alerts'	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-2g8f- gjrr-x5cg	A-SAL-SUIT- 200624/525

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE- 2024-36408		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in Tree data entry point. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36409	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-pxq4- vw23-v73f	A-SAL-SUIT- 200624/526
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax messages count controller. Versions 7.14.4 and 8.6.1	N/A	A-SAL-SUIT- 200624/527

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a fix for this issue. CVE ID: CVE-2024-36410		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax displayView controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36411	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-9rvr- mcrf-p4p7	A-SAL-SUIT- 200624/528
Unrestricte d Upload of File with Dangerous Type	10-Jun-2024	8.8	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in uploaded file verification in products allows for remote code execution. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-c82f- 58jv-jfrh	A-SAL-SUIT- 200624/529

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID: CVE- 2024-36415			
N/A	10-Jun-2024	7.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a deprecated v4 API example with no log rotation allows denial of service by logging excessive data. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36416	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-jrpp- 22g3-2j77	A-SAL-SUIT- 200624/530	
Weak Password Recovery Mechanism for Forgotten Password	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, a user password can be reset from an unauthenticated attacker. The attacker does not get access to the new password. But this can be annoying for the user. This attack is also dependent on some password	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-6p2f- wwx9-952r	A-SAL-SUIT- 200624/531	

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset functionalities being enabled. It also requires the system using php 7, which is not an officially supported version. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE- 2024-36407		
Server- Side Request Forgery (SSRF)	10-Jun-2024	6.5	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the connectors file verification allows for a server-side request forgery attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36414	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-wg74- 772c-8gr7	A-SAL-SUIT- 200624/532
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the	https://github.c om/salesagility /SuiteCRM/sec urity/advisories /GHSA-ph2c- hvvf-r273	A-SAL-SUIT- 200624/533

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: sc_f	ilechecker_pro	oject	import module error view allows for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue. CVE ID: CVE-2024-36413		
Product: sc_					
Affected Vers	sion(s): * Up to	(including	g) 0.6		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Siteclean SC filechecker allows Path Traversal, File Manipulation.This issue affects SC filechecker: from n/a through 0.6. CVE ID: CVE- 2024-35743	N/A	A-SCSC_F- 200624/534
Vendor: sea	cms				
Product: sea					
Affected Vers	sion(s): 12.9				
N/A	10-Jun-2024	9.1	SeaCMS 12.9 has a file deletion vulnerability via admin_template.ph p. CVE ID: CVE-2024-31611	N/A	A-SEA-SEAC- 200624/535
Vendor: sec	uronyov				

	CVSSv3 Scoring Scale
×	* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Product: multi-factor_authentication_solutions										
Affected Version(s): * Up to (excluding) 9.4.514										
Cleartext Transmissi on of Sensitive Informatio n	10-Jun-2024	7.5	Multiple injections vulnerabilities exist in SecurEnvoy MFA before 9.4.514 due to improper validation of user- supplied input. An unauthenticated remote attacker could exfiltrate data from Active Directory through blind LDAP injection attacks against the DESKTOP service exposed on the /secserver HTTP endpoint. This may include ms-Mcs- AdmPwd, which has a cleartext password for the Local Administrator Password Solution (LAPS) feature. CVE ID: CVE- 2024-37393	N/A	A-SEC-MULT- 200624/536					
Vendor: see										
Product: raf	-									
Affected Ver	sion(s): * Up to	(excludin								
Missing Authorizati on	10-Jun-2024	6.3	Missing Authorization vulnerability in RafflePress Giveaways and Contests by RafflePress.This	N/A	A-SEE-RAFF- 200624/537					
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-	8 8-9 9-10					

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Giveaways and Contests by RafflePress: from n/a through 1.12.4. CVE ID: CVE- 2024-4745		
Vendor: sel	ect-themes				
Product: sto	ockholm				
Affected Ver	sion(s): * Up to	(excluding	g) 9.7		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	9.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6. CVE ID: CVE- 2024-34551	N/A	A-SEL-STOC- 200624/538
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	8.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm allows PHP Local File Inclusion.This issue affects Stockholm: from n/a through 9.6.	N/A	A-SEL-STOC- 200624/539

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2024-34552		
Product: sto	ockholm_core				
Affected Ver	sion(s): * Up to	(excluding	g) 2.4.2		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	8.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Select-Themes Stockholm Core allows PHP Local File Inclusion.This issue affects Stockholm Core: from n/a through 2.4.1. CVE ID: CVE- 2024-34554	N/A	A-SEL-STOC- 200624/540
Vendor: sen	dinblue				
Product: ne	wsletter_smt	p_emai	l_marketing_and_sub	scribe	
Affected Vers	sion(s): * Up to	(excluding	g) 3.1.78		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue allows Reflected XSS.This issue affects Newsletter, SMTP, Email marketing and Subscribe	N/A	A-SEN-NEWS- 200624/541

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
			forms by Sendinblue: from n/a through 3.1.77. CVE ID: CVE- 2024-35668								
Vendor: sina	aextra										
Product: sina_extension_for_elementor											
Affected Vers	sion(s): * Up to	(excluding	g) 3.5.2								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SinaExtra Sina Extension for Elementor allows PHP Local File Inclusion.This issue affects Sina Extension for Elementor: from n/a through 3.5.1. CVE ID: CVE- 2024-34384											
Vendor: soft	tlabbd										
Product: int	egrate_google	_drive									
Affected Vers	sion(s): * Up to	(excluding									
Improper Authentica tion	04-Jun-2024	9.8	Broken Authentication vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.93. CVE ID: CVE- 2024-35670	N/A	A-SOF-INTE- 200624/543						
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7	7-8 8-9 9-10						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Product: up	load_fields_for	_wpform	S							
Affected Version(s): * Up to (including) 1.0.2										
Missing Authorizati on	09-Jun-2024	Missing Authorization vulnerability in SoftLab Upload Fields for WPForms.This		N/A	A-SOF-UPLO- 200624/544					
Vendor: Sol	arwinds									
Product: ser	rv-u									
Affected Ver	sion(s): * Up to	(excluding	g) 15.4.2							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-2024	7.5	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive	https://www.so larwinds.com/t rust- center/security- advisories/CVE- 2024-28995	A-SOL-SERV- 200624/545					

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 on the host machine.		
			CVE ID: CVE- 2024-28995		
Affected Ver	sion(s): 15.4.2				l
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Jun-2024	7.5	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine. CVE ID: CVE-2024-28995	https://www.so larwinds.com/t rust- center/security- advisories/CVE- 2024-28995	A-SOL-SERV- 200624/546
Product: sol	larwinds_platf	orm			
	sion(s): * Up to		g) 2024.2		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-Jun-2024	8.1	The SolarWinds Platform was determined to be affected by a SWQL Injection Vulnerability. Attack complexity is high for this vulnerability. CVE ID: CVE-	https://www.so larwinds.com/t rust- center/security- advisories/CVE- 2024-28996	A-SOL-SOLA- 200624/547
Concurrent Execution	04-Jun-2024	8.1	The SolarWinds Platform was	https://www.so larwinds.com/t	A-SOL-SOLA- 200624/548
using Shared CVSSv3 Scoring	Scale 0-1	1-2 2	determined to be affected by a Race -3 3-4 4-5	rust- center/security-	·

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchroniz ation ('Race Condition')			Condition Vulnerability affecting the web console. CVE ID: CVE- 2024-28999	advisories/CVE- 2024-28999	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	4.8	The SolarWinds Platform was determined to be affected by a stored cross-site scripting vulnerability affecting the web console. A high- privileged user and user interaction is required to exploit this vulnerability. CVE ID: CVE- 2024-29004	https://www.so larwinds.com/t rust- center/security- advisories/CVE- 2024-29004	A-SOL-SOLA- 200624/549
Vendor: spi					
	iffy_calendar	<i>C</i> 1 1:) 4 O 1 1		
Affected Ver	sion(s): * Up to	(excluding			T
Missing Authorizati on	04-Jun-2024	6.3	Missing Authorization vulnerability in Spiffy Plugins Spiffy Calendar.This issue affects Spiffy Calendar: from n/a through 4.9.10.	N/A	A-SPI-SPIF- 200624/550
			CVE ID: CVE- 2024-30528		
Product: wp	_flow_plus				
Affected Ver	sion(s): * Up to	(excluding	g) 5.2.3		
Improper Neutralizat ion of Input During	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation	N/A	A-SPI-WP_F- 200624/551

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
			Strategery Migrations: from n/a through 1.0. CVE ID: CVE- 2024-35745								
Vendor: stylemixthemes											
Product: me	ega_menu										
Affected Ver	sion(s): * Up to	(excludin	g) 2.3.13								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	9.8	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in StylemixThemes MegaMenu allows PHP Local File Inclusion.This issue affects MegaMenu: from n/a through 2.3.12. CVE ID: CVE- 2024-35677	N/A	A-STY-MEGA- 200624/554						
Vendor: sur	nmar										
Product: me	entor										
Affected Ver	sion(s): 3.83.35										
Deserializa tion of Untrusted Data	06-Jun-2024	9.8	Untrusted data deserialization vulnerability has been found in Mentor - Employee Portal, affecting version 3.83.35. This vulnerability could allow an attacker to execute arbitrary code, by injecting a malicious payload	N/A	A-SUM-MENT- 200624/555						

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	cription & CVE ID Patch		
			into the "ViewState" field. CVE ID: CVE-2024-5675			
Vendor: Sys	aid					
Product: sys	said					
Affected Ver	sion(s): * Up to	(including	g) 23.3.38			
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2024	9.8	SysAid - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CVE ID: CVE- 2024-36393	N/A	A-SYS-SYSA- 200624/556	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	06-Jun-2024	9.8	SysAid - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') CVE ID: CVE- 2024-36394	N/A	A-SYS-SYSA- 200624/557	
Vendor: the	mehigh					
Product: ch	eckout_field_e	ditor_for_	woocommerce			
Affected Ver	sion(s): * Up to	(excluding	g) 3.6.3			
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	9.1	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ThemeHigh Checkout Field	N/A	A-THE-CHEC- 200624/558	

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID							
			Editor for WooCommerce (Pro) allows Functionality Misuse, File Manipulation.This issue affects Checkout Field Editor for WooCommerce (Pro): from n/a through 3.6.2. CVE ID: CVE-2024-35658									
Vendor: the	meisle											
Product: pro	oduct_addons_	\&_fields	_for_woocommerce									
Affected Vers	sion(s): * Up to	(excluding	g) 32.0.21									
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	10-Jun-2024	5.3	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Themeisle PPOM for WooCommerce allows Code Inclusion.This issue affects PPOM for WooCommerce: from n/a through 32.0.20. CVE ID: CVE- 2024-35728	N/A	A-THE-PROD- 200624/559							
Vandor, the	mokraft	Vendor: themekraft										
Product: bu		(including	g) 2.8.9									
Product: bu	ddyforms	(including	The BuddyForms plugin for	N/A	A-THE-BUDD- 200624/560							

Weakness	Publish Date	CVSSv3	Description &	CVE ID		Patch		NCIIP	C ID		
ly Random Values			WordPress is vulnerable to Email Verification Bypass in all versions up to, and including, 2.8.9 via the use of an insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification. CVE ID: CVE-2024-5149								
Product:											
buddypress_woocommerce_my_account_integrationcreate_woocommerce_member_pag es											
Affected Vers	sion(s): * Up to	(excludin	g) 3.4.20								
Missing Authorizati on	10-Jun-2024	8.8	Missing Authorization vulnerability ThemeKraft WooBuddy.T issue WooBuddy: n/a through CVE ID: 2024-35726	in This affects from 3.4.19.	N/A			A-THE-B 200624/			
Vendor: the	mesflat										
Product: the	emesflat_addo	ns_for_el	ementor								
Affected Vers	sion(s): * Up to	(including	g) 2.1.2								
Improper Neutralizat ion of Input During Web Page Generation	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesflat					A-THE-T 200624/			
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Themesflat Addons For Elementor allows Stored XSS.This issue affects Themesflat Addons For Elementor: from n/a through 2.1.2. CVE ID: CVE- 2024-35666		
Vendor: the	meum			l	<u>'</u>
Product: tut	tor_lms				
Affected Vers	sion(s): * Up to	(excluding	g) 2.7.2		
Authorizati on Bypass Through User- Controlled Key	07-Jun-2024	4.3	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.7.1 via the 'attempt_delete' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Instructor-level access and above, to delete arbitrary quiz attempts. CVE ID: CVE- 2024-5438	https://plugins. trac.wordpress. org/changeset/ 3098465/	A-THE-TUTO- 200624/563
	newsletterplu	gın			
Product: ne	wsletter				

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ons_check function. This makes it possible for unauthenticated attackers to extract basic information about website users, including their emails CVE ID: CVE-2024-5483	his makes it ossible for nauthenticated ctackers to extract asic information bout website sers, including teir emails VE ID: CVE-	
Vendor: ticl	kera				
Product: tic	kera				
Affected Ver	sion(s): * Up to	(excludin	g) 3.5.2.7		
Missing Authorizati on	10-Jun-2024	8.8	Missing Authorization vulnerability in Tickera.This issue affects Tickera: from n/a through 3.5.2.6. CVE ID: CVE- 2024-35729	N/A	A-TIC-TICK- 200624/566
Vendor: tnb	mobil				
Product: co	ckpit				
Affected Ver	sion(s): * Up to	(excludin	g) 0.251.1		
N/A	05-Jun-2024	7.5	Inclusion of Sensitive Information in Source Code vulnerability in TNB Mobile Solutions Cockpit Software allows Retrieve Embedded Sensitive Data.This issue affects Cockpit Software: before v0.251.1.	N/A	A-TNB-COCK- 200624/567

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID							
			CVE ID: CVE- 2024-1272									
Vendor: trik	pe29											
Product: ch	Product: checkmk											
Affected Version(s): 2.3.0												
Improper Restriction of Excessive Authentica tion Attempts	10-Jun-2024	7.5	Improper restriction of excessive authentication attempts with two factor authentication methods in Checkmk 2.3 before 2.3.0p6 facilitates brute-forcing of second factor mechanisms. CVE ID: CVE-2024-28833	https://checkm k.com/werk/16 830	A-TRI-CHEC- 200624/568							
	imited-elemer											
			lementor_\(free_wid	gets_addons_t	emplates\)							
Affected Ver	sion(s): * Up to	(excluding			I							
Missing Authorizati on	05-Jun-2024	8.8	Missing Authorization vulnerability in Unlimited Elements Unlimited Elementor (Free Widgets, Addons, Templates).This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from	N/A	A-UNL-UNLI- 200624/569							

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
----------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	n/a through 1.5.109. CVE ID: CVE-2024-35674 The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to blind SQL Injection via the 'data[addonID]' parameter in all versions up to, and including, 1.5.109	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	06-Jun-2024	8.8	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 Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. CVE ID: CVE-2024-5329	https://plugins. trac.wordpress. org/changeset/ 3097249/#file6	A-UNL-UNLI- 200624/570
Vendor: upu Product: upu	ınzipper_proje unzipper	ct			
CVSSv3 Scoring * stands for all ve		1-2 2	3-4 4-5	5-6 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): * Up to	(including	g) 1.0.0		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Jun-2024	6.5	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ravidhu Dissanayake Upunzipper allows Path Traversal, File Manipulation.This issue affects Upunzipper: from n/a through 1.0.0. CVE ID: CVE- 2024-35744	N/A	A-UPU-UPUN- 200624/571
Vendor: use	rproplugin				
Product: use	erpro				
Affected Vers	sion(s): * Up to	(excluding	g) 5.1.9		
N/A	04-Jun-2024	9.8	Improper Privilege Management vulnerability in DeluxeThemes Userpro allows Privilege Escalation.This issue affects Userpro: from n/a through 5.1.8. CVE ID: CVE-	N/A	A-USE-USER- 200624/572
			2024-35700		
Vendor: van	ıyukov				
Product: ma	ırket_exporter				
Affected Vers	sion(s): * Up to	(excluding	g) 2.0.20		
Improper Limitation of a Pathname	07-Jun-2024	8.1	The Market Exporter plugin for WordPress is vulnerable to	https://plugins. trac.wordpress. org/changeset/ 3098360/mark	A-VAN-MARK- 200624/573
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

to a Restricted Directory ('Path			,		
Traversal')			unauthorized loss of data due to a missing capability check on the 'remove_files' function in all versions up to, and including, 2.0.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to use path traversal to delete arbitrary files on the server. CVE ID: CVE-2024-5637	et- exporter/trunk /includes/class- restapi.php	
Vendor: Vide	eowhisper				
Product: pict	ture_gallery				
Affected Vers	sion(s): * Up to	(excluding	g) 1.5.12		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VideoWhisper Picture Gallery allows Stored XSS.This issue affects Picture Gallery: from n/a through 1.5.11. CVE ID: CVE- 2024-34759	N/A	A-VID-PICT- 200624/574
Vendor: visu	alcomposer				
Product: visi	ual_composer	_website_	builder		

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	C ID
Affected Vers	sion(s): * Up to	(excluding	g) 45.9.0		1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	5.4	Improper Neutraliza Input Dur Page Ge (XSS or 'C Scripting') vulnerability visual composer allows XSS.This affects Composer Builder: f through 45 CVE ID: 2024-356	ing Web eneration Cross-site ity in poser.Co composer Builder Stored issue Visual Website rom n/a 5.8.0.	N/A			A-VIS-VIS 200624/	
Vendor: viz									
Product: na	no_id								
Affected Vers	sion(s): * Up to	(excluding	g) 0.4.0						
Insufficient Entropy	04-Jun-2024	9.8	nano-id is string ID g for Rust. versions nano-id incorrectly generated a reduced of set in 'nano_id::b' and 'nano_id::b' functions. Specifically 'base62' used a charof 32 instead intended	generator Affected of the crate IDs using character the base62` ase58` y, the function	om/v rs/na id/co 2277 929b 70ac9 https om/v rs/na id/se isorie	nno- mmit/a 2b2f1ce 5b81ece 9d3ab23 ://githu riz- nno- curity/a es/GHSA	90 238 cc6 3, ib.c	A-VIZ-NA 200624/	
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Neutralizat of Input O4-Jun-2024 6.1 Neutralization of Input During Web N/A 200624/577	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of 16 symbols instead of the intended 58 symbols. Additionally, the 'nano_id::gen' macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): *Up to (excluding) 2.3.2 Improper Neutralization of Input During Web M/A A-VOL-EVEN-200624/577				`base58` function		
instead of the intended 58 symbols. Additionally, the 'nano_id::gen' macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				used a character set		
intended 58 symbols. Additionally, the 'nano_id::gen' macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Mfected Version(s): * Up to (excluding) 2.3.2 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				of 16 symbols		
symbols. Additionally, the 'nano_id::gen' macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralization of Input During Web N/A A-VOL-EVEN_200624/577				instead of the		
Additionally, the 'namo_id::gen' macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'namo_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 mproper Neutralization of Input During Web N/A A-VOL-EVEN_200624/577				intended 58		
`nano_id::gen` macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that `nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security- sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 mproper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN- 200624/577				symbols.		
macro is also affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'nano.id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 mproper Neutralizat				Additionally, the		
affected when a custom character set that is not a power of 2 in size is specified. It should be noted that 'nano.id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat of Input During Web N/A A-VOL-EVEN-200624/577 Input During Web				`nano_id::gen`		
custom character set that is not a power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 mproper Neutralizat of Input During Web N/A A-VOL-EVEN_200624/577 Inproper Neutralization of Input During Web				macro is also		
set that is not a power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 O4-Jun-2024 O4-Jun-2024 O6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				affected when a		
power of 2 in size is specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat of Input During Web N/A A-VOL-EVEN-200624/577				custom character		
specified. It should be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 O4-Jun-2024 O4-Jun-2024 O4-Jun-2024 OA-VOL-EVEN-200624/577 Improper Neutralization of Input During Web				set that is not a		
be noted that 'nano_id::base64' is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web				power of 2 in size is		
nano_id::base64` is not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 O4-Jun-2024 O4-Jun-2024 O5.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				specified. It should		
not affected by this vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input 04-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				be noted that		
vulnerability. This can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 mproper Neutralizat on of Input My/A A-VOL-EVEN-200624/577 Improper Neutralization of Input During Web				`nano_id::base64` is		
can result in a significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE_2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 mproper Neutralizat on of Input M/A A-VOL-EVEN-200624/577 Improper Neutralization of Input During Web				not affected by this		
significant reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security- sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input N/A A-VOL-EVEN- 200624/577				vulnerability. This		
reduction in entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				can result in a		
entropy, making the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralization of Input O4-Jun-2024 O4-Ju				significant		
the generated IDs predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralization of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				reduction in		
predictable and vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				entropy, making		
vulnerable to brute-force attacks when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				the generated IDs		
brute-force attacks when the IDs are used in security- sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralization of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN- 200624/577				predictable and		
when the IDs are used in security-sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				vulnerable to		
used in security- sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input Well During Web A-VOL-EVEN- 200624/577				brute-force attacks		
sensitive contexts such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input A-VOL-EVEN- 200624/577				when the IDs are		
such as session tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				used in security-		
tokens or unique identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				sensitive contexts		
identifiers. The vulnerability is fixed in 0.4.0. CVE ID: CVE-2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024				such as session		
vulnerability is fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN- 200624/577				tokens or unique		
fixed in 0.4.0. CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web A-VOL-EVEN- 200624/577						
CVE ID: CVE- 2024-36400 Vendor: vollstart Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024				,		
Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				fixed in 0.4.0.		
Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577				CVE ID: CVE-		
Product: event_tickets_with_ticket_scanner Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web A-VOL-EVEN-200624/577						
Affected Version(s): * Up to (excluding) 2.3.2 Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web N/A A-VOL-EVEN-200624/577	Vendor: vol	lstart				
Improper Neutralizat on of Input O4-Jun-2024 6.1 Improper Neutralization of Input During Web A-VOL-EVEN-200624/577	Product: ev	ent_tickets_wit	th_ticket_	scanner		
Neutralizat of Input O4-Jun-2024 6.1 Neutralization of Input During Web N/A 200624/577	Affected Ver	sion(s): * Up to	(excluding	g) 2.3.2		
Neutralizat 04-Jun-2024 6.1 Neutralization of N/A 200624/577 Input During Web	Improper			Improper		A-VOL-EVEN-
on of Input Input During Web	Neutralizat	04-Jun-2024	6.1	Neutralization of	N/A	
CVSSv2 Scoring Scale 0.1 1.2 2.2 2.4 4.5 5.6 6.7 7.0 0.0	ion of Input			Input During Web		200021/3//
CV 23 Y 2 SUULIUS SUULE UT 1-7 7-5 5-4 4-7 5-6 6-7 7-8 8-9 9-111	CVSSv3 Scoring	Scale 0-1	1-2 2	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')			Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saso Nikolov Event Tickets with Ticket Scanner allows Reflected XSS.This issue affects Event Tickets with Ticket Scanner: from n/a through 2.3.1. CVE ID: CVE-2024-35652		
Vendor: wb	comdesigns				
	stom_font_uplo				
Affected Ver	sion(s): * Up to	(excluding			
Missing Authorizati on	06-Jun-2024	4.3	The Wbcom Designs – Custom Font Uploader plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'cfu_delete_customf ont' function in all versions up to, and including, 2.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete any custom font. CVE ID: CVE- 2024-5489	https://plugins. trac.wordpress. org/changeset/ 3097373/	A-WBC-CUST- 200624/578

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wea	avertheme				
Product: we	aver_xtreme_t	heme_su	pport		
Affected Vers	sion(s): * Up to	(excluding	g) 6.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Weaver Xtreme Theme Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's div shortcode in all versions up to, and including, 6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4939	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&new=30 95286%40wea verx-theme- support%2Ftru nk&old=301794 3%40weaverx- theme- support%2Ftru nk&sfp_email= &sfph_mail=	A-WEA-WEAV- 200624/579
Product: au	dimexee				
Affected Vers	sion(s): 15.1.2				
Improper Neutralizat ion of Input During Web Page Generation	04-Jun-2024	5.4	Cross Site Scripting vulnerability in audimex audimexEE v.15.1.2 and fixed in 15.1.3.9 allows a	N/A	A-WEB-AUDI- 200624/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to execute arbitrary code via the service, method, widget_type, request_id, payload parameters. CVE ID: CVE-2024-30889		
Vendor: we	bsupporter_fil	ter_custo	m_fields_\&_taxonon	nies_light_project	
Product: we	ebsupporter_fi	ter_custo	om_fields_\&_taxono	mies_light	
Affected Ver	sion(s): * Up to	(including	g) 1.05		
Missing Authorizati on	09-Jun-2024	8.8	Authorization vulnerability in Websupporter Filter Custom Fields & Taxonomies Light.This issue affects Filter Custom Fields & Taxonomies Light: from n/a through 1.05. CVE ID: CVE- 2024-32081	N/A	A-WEB-WEBS- 200624/581
Vendor: we	stguardsolutio	ns			
Product: ws					
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Formula Elements in a CSV File	07-Jun-2024	8.8	The WS Form LITE plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.9.217. This allows unauthenticated attackers to embed	https://plugins. trac.wordpress. org/changeset? sfp_email=&sfp h_mail=&repon ame=&old=309 8265%40ws- form&new=309 8265%40ws-	A-WES-WS_F- 200624/582

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration. CVE ID: CVE-2023-5424	form&sfp_email =&sfph_mail=	
Vendor: wil	lnorris				
Product: op					
Affected Ver	sion(s): * Up to	(excluding	g) 1.11.3		
N/A	06-Jun-2024	5.3	The Open Graph plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.11.2 via the 'opengraph_default_description' function. This makes it possible for unauthenticated attackers to extract sensitive data including partial content of password-protected blog posts. CVE ID: CVE-2024-5615	https://plugins. trac.wordpress. org/changeset/ 3097574/	A-WIL-OPEN- 200624/583

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wo	bbie				
Product: mo	ollie_forms				
Affected Ver	sion(s): * Up to	(excluding	g) 2.6.14		
Cross-Site Request Forgery (CSRF)	05-Jun-2024	4.3	The Mollie Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.13. This is due to missing or incorrect nonce validation on the duplicateForm() function. This makes it possible for unauthenticated attackers to duplicate forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. CVE ID: CVE-2024-2368	https://plugins. trac.wordpress. org/changeset/ 3097426/molli e-forms	A-WOB-MOLL- 200624/584
		footer by	ıilder_for_elementor		
	sion(s): * Up to				
Anicoleu vel		CACIUUIII			
Improper Neutralizat ion of Input During Web Page Generation	05-Jun-2024	5.4	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site	https://plugins. trac.wordpress. org/changeset/ 3097085/#file9	A-W00-B00S- 200624/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting via the 'size' parameter in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-5006		
Vendor: wo	w-company				
	sy_digital_dow sion(s): * Up to		g) 1.0.2		
Inclusion of Functionali ty from Untrusted Control Sphere	04-Jun-2024	9.8	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Wow-Company Easy Digital Downloads – Recent Purchases allows PHP Remote File Inclusion.This issue affects Easy Digital Downloads – Recent Purchases:	N/A	A-WOW-EASY- 200624/586

CVSSv3 Scoring Scale 0-1	1-2 2-	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 n/a through 1.0.2. CVE ID: CVE-2024-35629		
Product: wo	ocommerce	recent_p	urchases		
Affected Ver	sion(s): * Up to	(including	g) 1.0.1		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Jun-2024	4.9	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Wow-Company Woocommerce – Recent Purchases allows PHP Local File Inclusion.This issue affects Woocommerce – Recent Purchases: from n/a through 1.0.1. CVE ID: CVE-	N/A	A-WOW-WOOC- 200624/587
Vendor: wp	attiro		2024-35634		
Product: att					
	sion(s): * Up to	(excludin	g) 1.9.3		
Missing Authorizati on	05-Jun-2024	4.3	The Gutenberg Blocks and Page Layouts – Attire Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the disable_fe_assets function in all	https://plugins. trac.wordpress. org/changeset/ 3085600/attire - blocks/trunk/a dmin/AttireBlo cksSettings.php ?old=2996841& old_path=attire- blocks%2Ftrun k%2Fadmin%2	A-WPA-ATTI- 200624/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 1.9.2. This makes it possible for authenticated attackers, with subscriber access or above, to change the plugin's settings. Additionally, no nonce check is performed resulting in a CSRF vulnerability. CVE ID: CVE-2024-4088	FAttireBlocksSe ttings.php	
Vendor: wp	developer				
Product: em	bedpress				
Affected Vers	sion(s): * Up to	(excluding	g) 3.9.9		
Missing Authorizati on	09-Jun-2024	9.8	Missing Authorization vulnerability in WPDeveloper EmbedPress.This issue affects EmbedPress: from n/a through 3.9.8. CVE ID: CVE- 2024-31284	N/A	A-WPD-EMBE- 200624/589
Affected Vers	sion(s): * Up to	(excluding	g) 4.0.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed https://plugitrac.wordpress Audios, Maps & org/changes Embed Any Documents in Gutenberg & Elementor plugin		A-WPD-EMBE- 200624/590
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CV	E ID	Patch	NCIIP	CID	
			for WordPress vulnerable Stored Cross- Scripting via 'url' attribution within the pluge EmbedPress widget in versions up to, including, 4.0.1 to insufficient in sanitization output escaping user suppattributes. makes it poss for authentica attackers, versions and about the inject arbition web scripts pages that execute whenev user accesses injected page.	to -Site the bute gin's PDF all and due nput and g on blied This sible ated with el oove, crary in will ver a				
Product: ess	sential_addons	_for_ele	mentor					
Affected Vers	sion(s): * Up to	(excludii	ng) 5.9.23					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-Jun-2024	5.4	The Esser Addons Elementor – If Elementor Templates, Widgets, Kits WooCommerce Builders plugin WordPress vulnerable Stored Cross- Scripting via 'get_manual_cale	for Best http: trace org, 309 is to Site the	os://plugi .wordpre /changeso 7900/	ess.	A-WPD-E 200624/	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ar_events' function in all versions up to, and including, 5.9.22 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-5188		
Vendor: wp	downloadman	ager			
Product: do	wnload_manag	ger			
Affected Ver	sion(s): * Up to	(excludin	g) 3.2.94		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-Jun-2024	5.4	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm_modal_login_form' shortcode in all versions up to, and including, 3.2.93 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible	https://plugins. trac.wordpress. org/changeset/ 3096459/	A-WPD-DOWN- 200624/592

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. CVE ID: CVE-2024-4001		
Vendor: wp	factory				
Product: pr	oducts_order	_\&_cust	omers_export_for_wo	oocommerce	
Affected Ver	sion(s): * Up to	(excluding	g) 2.0.9		
Missing Authorizati on	09-Jun-2024	9.8	Missing Authorization vulnerability in WPFactory Products, Order & Customers Export for WooCommerce.Thi s issue affects Products, Order & Customers Export for WooCommerce: from Na through 2.0.8. CVE ID: CVE- 2024-31276	N/A	A-WPF-PROD- 200624/593
Vendor: wp	foxly				
Product: ad	foxly				
Affected Ver	sion(s): * Up to	(including	g) 1.8.5		
Missing Authorizati on	09-Jun-2024	9.8	Missing Authorization vulnerability in AdFoxly AdFoxly – Ad Manager, AdSense Ads &		A-WPF-ADFO- 200624/594

1-2

3-4

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ads.Txt.This issue affects AdFoxly – Ad Manager, AdSense Ads & Ads.Txt: from n/a through 1.8.5. CVE ID: CVE-2024-34802		
Vendor: wp					
	ovivid_backup_		=		
Affected Ver	sion(s): * Up to	(excluding			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-Jun-2024	6.1	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPvivid Team WPvivid Backup for MainWP allows Reflected XSS.This issue affects WPvivid Backup for MainWP: from n/a through 0.9.32. CVE ID: CVE- 2024-35664	N/A	A-WPV-WPVI- 200624/595
Vendor: xoo	otix			l	<u>'</u>
Product: log	gin\/signup_po	pup			
Affected Ver	sion(s): From (i	ncluding)	2.7.1 Up to (excluding	g) 2.7.3	
Missing Authorizati on	06-Jun-2024	4.3	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized access of data due	https://plugins. trac.wordpress. org/changeset/ 3093994/	A-X00-L0GI- 200624/596

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	De	scription	& CVE ID)	Patch		NCIII	PC ID
	h_woocomme	-	the 'ex fur 2.7 ma for att Su acc to op sit CV 20	port_set nction in 7.1 to 2. akes it authorizers, bscriber cess and read itions on es. E ID: 24-566	tings' version: 7.2. This possible enticated with -level d above arbitrary affected	s s s e e d d n				
Affected Vers	sion(s): * Up to	(excludi	ng) 4.	9.3						
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	10-Jun-2024	5.3	Ne Sp Ou Do Co ('In vu YI' Wo Pro all Inj aff Wo 4.9	ooCommoduct ows ection.T ects ooCommoduct om n/a 0.2.	ments in ed by a m t) ty in YITH erce Add-Ons through	n a l a l a l a l a l a l a l a l a l a	A		A-YIT-Y 200624,	
Vendor: zor								_		
Product: ad	vanced_local_p	oickup_f	or_w	oocomn	ierce					
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Affected Version(s): * Up to (excluding) 1.6.3									
Pickup for WooCommerce: from n/a through 1.6.2.		N/A	A-ZOR-ADVA- 200624/598						
		2024-31283							
		Hardware							
	01								
sion(s): -									
05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/599					
05-Jun-2024	7.8	Replay Attack in ABB, Busch- Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/600					
	09-Jun-2024 B ma310010b00 sion(s): -	09-Jun-2024 9.8	Sion(s): * Up to (excluding) 1.6.3 Missing Authorization vulnerability in zorem Advanced Local Pickup for WooCommerce. Thi s issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.6.2. CVE ID: CVE-2024-31283	Missing Authorization vulnerability in zorem Advanced Local Pickup for WooCommerce:This s issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.6.2. CVE ID: CVE- 2024-31283 Hardware B ma310010b0001 sion(s):- FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008 Replay Attack https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=n&Docume ntPartId=&Acti on=Launch 7.8 Replay Attack https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=n&Docume ntPartId=&Acti on=Launch 7.8 Wissing Authorization WooCommerce:This s issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.6.2. CVE ID: CVE- 2024-31283 https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=n&Docume ntPartId=&Acti on=Launch					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local KNX Bus- System CVE ID: CVE- 2024-4009		
Product: 2tı	na310010b00	03			
Affected Vers	sion(s): -				
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/601
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX BusSystem CVE ID: CVE-2024-4009	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/602
	na310011b00	01			
Affected Vers	sion(s): -		EDCK Laslati ADD	latter of 1/221:	
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume	H-ABB-2TMA- 200624/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to local KNX Bus-System CVE ID: CVE- 2024-4008	ntPartId=&Acti on=Launch	
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch- Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus- System CVE ID: CVE- 2024-4009	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/604
	ma310011b00	02			
Affected Vers	sion(s): -		EDGILL 1: ADD		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/605
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	Replay Attack in ABB, Busch- Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			KNX telegram to local KNX Bus-System CVE ID: CVE-2024-4009			
Product: 2ti	ma310011b00	03				
Affected Ver	sion(s): -					
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/607	
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bussystem CVE ID: CVE-2024-4009	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	H-ABB-2TMA- 200624/608	
Vendor: Mitel						
Affected Vers	-					
Improper Neutralizat ion of Special	09-Jun-2024	8.8	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x	N/A	H-MIT-6869- 200624/609	

0-1

1-2

2-3

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 a Command ('Comman d Injection')			through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in the hostname parameter. CVE ID: CVE- 2024-37569		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-Jun-2024	8.8	On Mitel 6869i 4.5.0.41 devices, the Manual Firmware Update (upgrade.html) page does not perform sanitization on the username and path parameters (sent	N/A	H-MIT-6869- 200624/610

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

by an authenticated user) before appending flags to the busybox ftpget command. This leads to \$() command execution. CVE ID: CVE-2024-37570 Vendor: Samsung Product: exynos_1080 Affected Version(s):- An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, w930, Modem 5123, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	Weakness Pu	ublish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-				user) before appending flags to the busybox ftpget command. This leads to \$() command execution. CVE ID: CVE-		
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-	Vendor: Samsu	ng				
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem Com/support/q uality-support/productors. Samsung com/support/q uality-support/productors. Support/productors.	Product: exyno	s_1080				
N/A O4-Jun-2024 7.5 discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-	Affected Version	ı(s): -				
	N/A 04	ŀ-Jun-2024	7.5	discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-	ductor.samsung .com/support/q uality- support/produc t-security-	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/612
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/613

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/614
Product: ex	ynos_1280				
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor,	https://semicon ductor.samsung .com/support/q uality-	H-SAM-EXYN- 200624/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE- 2024-29152	support/produc t-security- updates/	
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/616

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description	& CVE ID		Patch		NCIIP	C ID
			baseband a does not check specified RRC. This to discloss sensitive information CVE ID: 2023-4992	states by the can lead sure of cVE-					
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issued discovered Samsung Processor, Automotive Processor, Wearable Processor, Modem 980, 990 1080, 2100 1280, 1380 9110, Exynos 5123, Modem 53 Exynos T5123. baseband does not check form specified RRC. This to a latencryption CVE ID: 2023-4992	and Exynos (a), 850, 0, 2200, 0, 1330, W920, Modem Exynos (a), and Auto The software properly (at types by the can lead ack of (a).	ducto .com/ uality support-secu	ort/pro urity-	ing t/q	H-SAM-E 200624/	
N/A	05-Jun-2024	5.3	An issue discovered Samsung Processor, Automotive Processor,	in Mobile	ducto .com/ uality	://semi or.samsi /suppor ort/pro	ing t/q	H-SAM-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Modem Exynos 9820, 9825, 980, 9850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE_2023-50803	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung Mobile Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1080, 2100				9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.		
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung Hobile Processor, and https://semicon ductor.samsung .com/support/q uality-support/produc t-security-updates/	Product: ex	ynos_1330		2023-50803		
M/A O4-Jun-2024 7.5 discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 2200, 2400, 9110, W920, 2400, 9110, W	Affected Ver	sion(s): -				
				discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration	ductor.samsung .com/support/q uality- support/produc t-security- updates/	200624/619

^{*} stands for all versions

Missing Encryption of Sensitive Data O5-Jun-2024 7.5 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Automotive Processor, S123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly updates/ Ut-SAM-EXYN 200624/621	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Automotive Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5123, Exynos Modem 5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Automotive Processor, Support/produc Samsung Mobile Processor, Automotive Support/produc Samsung Support/produc Support/Support/Support/Support/Support/Support/Support/Support/Support/Support/Support/Support/Support/Supp				lead to disclosure o sensitive information. CVE ID: CVE	f	
Missing Encryption of Sensitive Data discovered in Samsung Mobile Processor, Automotive Processor, Support/produc discovered in Samsung Mobile Processor, Automotive Support/produc Processor, Support/produc discovered in Samsung Mobile Processor, Support/produc processor, Support/produc	N/A	05-Jun-2024	7.5	discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850 1080, 2100, 2200 1280, 1380, 1330 9110, W920 Exynos Modem 5123, Exynos Modem 5300, and Exynos Automotive T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/620
Processor, and updates/ Modem Exynos	Encryption of Sensitive	05-Jun-2024	5.3	discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/621

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/622

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ynos_1380				
sion(s): -				
04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/623
05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/624
	ynos_1380 sion(s): - 04-Jun-2024	ynos_1380 sion(s): - 04-Jun-2024 7.5	ynos_1380 sion(s):- An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem Software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1080, 2100, 2200,	ynos_1380 sion(s):- An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, w930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Wearable Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 100, 2200,

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE- 2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/625

CVSSv3 Scoring Scale
* stands for all versions

N/A 05-Jun-2024 5.3 An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE 2023-56803 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Wearable Processor, Wearable Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband HTSs//semicon ductor.samsung com/support/q uality-support/product-security-updates/	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem 5123, Modem 5300, and Auto T5123. H-SAM-EXYN-200624/627 Automotive Processor, and Modem 5123, Modem 5300, and Auto T5123. Automotive Processor, and Automotive Processor, an	N/A	05-Jun-2024	5.3	discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	ductor.samsung .com/support/q uality- support/produc t-security-	
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. An issue was discovered in Samsung Mobile Processor, and Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123.	Duo du et. avi	.mag 2100		2023-50803		
N/A 04-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123.						
			7.5	discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123.	ductor.samsung .com/support/q uality- support/produc t-security-	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3		Description	& CVE ID		Patch		NCIIP	CID
			t F I I S ii	oftware of roperly tates spender of the configuration of the configuration of the configuration of the conformation of the con	check cified by (Radio Control) ration This can closure of n. CVE-					
N/A	05-Jun-2024	7.5	d d S S F A A F V V F F N G S T T d d d c c s F T T d d c c s S F T T T T T T T T T T T T T T T T T T	n issuiscovered amsung rocessor, utomotive rocessor, lodem 80, 996 080, 210 280, 138 110, xynos 123, lodem 53 xynos 5123. aseband oes not heck pecified RC. This of discloensitive informatio VE ID: 023-499	e and Exynos 0, 850, 00, 2200, W920, Modem Exynos 300, and Auto The software properly states by the can lead sure of n.	htt duc .co ual sup t-se upo	ps://semetor.sams m/suppo ity- pport/pro ecurity- lates/	sung ort/q	H-SAM-E 200624/	
Missing Encryption	05-Jun-2024	5.3	d	n issu iscovered amsung		duo	ps://sem ctor.sams n/suppo	sung	H-SAM-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE- 2023-49927	uality- support/produc t-security- updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/630

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803		
Product: ex Affected Ver					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/631
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor,	https://semicon ductor.samsung .com/support/q uality- support/produc	H-SAM-EXYN- 200624/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE- 2023-49928	t-security- updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/633

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927 An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5123	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 521, Modem 521, Modem 521, Modem 521, Modem 521, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803 Product: exynos_2400 Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos MyA O4-Jun-2024 An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos				RRC. This can lead to a lack of encryption. CVE ID: CVE-		
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos An issue was discovered in Samsung Mobile Processor, and Modem Exynos	N/A	05-Jun-2024	5.3	discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	ductor.samsung .com/support/q uality- support/produc t-security-	
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos An issue was discovered in Samsung Mobile Processor, and Modem Exynos https://semicon ductor.samsung .com/support/q uality-support/produc t-security-updates/	Product: ex	ynos_2400				
N/A 04-Jun-2024 7.5 discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos Miscovered in Samsung Mobile Processor, com/support/q uality-support/produc t-security-updates/ H-SAM-EXYN-200624/635	Affected Ver	sion(s): -				
	N/A	04-Jun-2024	7.5	discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	ductor.samsung .com/support/q uality- support/produc t-security-	

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152		
Product: ex	ynos_850		2021 23102		
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control)	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/636
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/637
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/638

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A CVSSv3 Scoring	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/639

CVSSv3 Scoring Scale
* stands for all versions

on(s): -	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semicon ductor.samsung .com/support/q uality- support/produc t-security-	H-SAM-EXYN- 200624/640
	7.5	discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband	ductor.samsung .com/support/q uality- support/produc	
04-Jun-2024	7.5	discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband	ductor.samsung .com/support/q uality- support/produc	
		software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	updates/	
os_980				
on(s): -				
04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/641
 D1	n(s): -	n(s): -	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and with the security-updates/ An issue was discovered in Samsung https://semicon ductor.samsung .com/support/q uality-support/produc t-security-updates/

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/642

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			to disclosure of sensitive information. CVE ID: CVE-2023-49928				
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/643		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/644		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	and The softv prop repla spec NAS Strat This denia		software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.		
			CVE ID: CVE- 2023-50803		
Product: ex					
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/645

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/646
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/647

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv	3	Description	& CVE ID		Patch			NCIIP	C ID
				software of properly replay properly pr	check rotection by the n-Access- module. lead to ervice. CVE-						
Product: ex	ynos_9825								<u> </u>		
Affected Vers	sion(s): -										
N/A	05-Jun-2024	7.5		An issuediscovered Samsung Processor, Automotive Processor, Wearable Processor, Modem 980, 990 1080, 210 1280, 138 9110, Exynos 5123, Modem 53 Exynos T5123. baseband does not check specified RRC. This to disclossensitive information CVE ID: 2023-4992	in Mobile and Exynos by 1330, and Auto The Software properly states by the can lead sure of the can lead of th	http duct .com ualit supp t-sec upd	port/pr curity- ates/	sung ort/q roduc	200	SAM-E 0624/	648
Missing Encryption	05-Jun-2024	5.3		An issu discovered		_	s://sen cor.sam			SAM-E 0624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	2	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	.com/support/q uality- support/produc t-security- updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/650

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803		
Product: ex	ynos_990				
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/651
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive	https://semicon ductor.samsung .com/support/q uality- support/produc	H-SAM-EXYN- 200624/652

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE- 2023-49928	t-security- updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/653

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/654
	ynos_auto_t51	23			
Affected Vers	sion(s): -			I	
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/655
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

980, 990, 850, 1080, 2100, 2200, 1280, 1330, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	Weakness	Publish Date	CVSSv3	Description	& CVE ID	Patch)	NCIIP	C ID
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by				1080, 2100 1280, 1380 2400, 9110 W930, 5123, Mode and Auto The b software d properly states spec the RRC Resource Reconfigura message. T lead to discissensitive information CVE ID:	0, 2200, 0, 1330, 0, W920, Modem em 5300, T5123. aseband loes not check cified by (Radio Control) ation This can losure of the CVE-				
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5123, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by	Droducti ov	unos modom l	- 122	2024-2915	52				
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by			3123						
			7.5	discovered Samsung Processor, Wearable Processor, Automotive Processor, Modem 980, 990 1080, 2100 1280, 1380 2400, 9110 W930, 5123, Mode and Auto The b software d properly states spec	in Mobile and Exynos 1, 850, 1, 2200, 1, 1330, 1, W920, 1, Modem 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,	ductor.san .com/supp uality- support/p t-security-	nsung oort/q roduc		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Des	cription	& CVE ID		Patch		NO	CIIP	CID
			Recomes lead sens info	onfigura sage. 1	This can losure of n. CVE-						
N/A	05-Jun-2024	7.5	Sam Proc Auto Proc Wea Proc 980 108 128 911 Exyr 512 Mod Exyr T51 base does chec spec RRC to sens	, 990 0, 210 0, 138 0, nos 3, lem 53 nos 23. eband s s not p ck cified disclos sitive rmation	in Mobile and Exynos , 850, 0, 2200, 0, 1330, W920, Modem Exynos 00, and Auto The software properly states by the can lead sure of	http: duct .com ualit supp t-sec upda	s://sem or.sams i/suppor y- port/pro curity- ates/	ung rt/q	H-SAN 20062		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An disc Sam Prod Auto	issue overed sung cessor, omotive cessor,	e was in Mobile	http: duct .com ualit	s://sem or.sams i/suppor y- port/pro	ung rt/q	H-SAN 20062		
CVSSv3 Scoring	Scale 0-1	1-2		rable 3-4	4-5	5-6	6-7	7-8	8-	0	9-10

^{*} stands for all versions

Weakness	ess Publish Date CVSS		Description & CVE ID	Patch	NCIIPC ID		
			Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	t-security- updates/			
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/659		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2023-50803		
Product: ex	ynos_modem_5	5300			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/660
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.		
			CVE ID: CVE- 2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/662

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/663
Product: exy	ynos_w920				
Affected Vers	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	H-SAM-EXYN- 200624/664
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8 8-9 9-10
* stands for all ve					

An issue was discovered in Samsung Mobile Processor, Automotive Pr	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung discovered in Samsung 40sovered in S				W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-		
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, w930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration						
N/A O4-Jun-2024 7.5 Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration Reconfiguration N/A O4-Jun-2024 7.5 Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, wupport/produc t-security-updates/ H-SAM-EXYN-200624/665	Affected vers	31011(3)		An issue was		
	N/A	04-Jun-2024	7.5	Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control)	ductor.samsung .com/support/q uality- support/produc t-security-	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to disclosure of sensitive information.		
			CVE ID: CVE- 2024-29152		
Vendor: Te	ndacn				
Product: o3	v2				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	04-Jun-2024	9.8	Tenda 03V2 v1.0.0.12(3880) was discovered to contain a Blind Command Injection via stpEn parameter in the SetStp function. This vulnerability allows attackers to execute arbitrary commands with root privileges. CVE ID: CVE-	N/A	H-TEN-03V2- 200624/666
Vendor: uni	iview		2024-36604		
	r301-04s2-p4				
Affected Ver					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	Uniview NVR301- 04S2-P4 is vulnerable to reflected cross-site scripting attack (XSS). An attacker could send a user a URL that if clicked on could execute malicious JavaScript in their browser. This vulnerability also requires	N/A	H-UNI-NVR3- 200624/667

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication before it can be exploited, so the scope and severity is limited. Also, even if JavaScript is executed, no additional benefits are obtained. CVE ID: CVE- 2024-3850		
Vendor: vw					
	charger_conne	ect			
Affected Ver	sion(s): -				
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass	N/A	H-VW-ID.C- 200624/668

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. CVE ID: CVE-2024-5684		
	charger_pro				
Affected Ver	sion(s): -				
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated	N/A	H-VW-ID.C- 200624/669

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can exploit this vulnerability to bypass the authentication mechanism. CVE ID: CVE-2024-5684		
			Operating System		
Vendor: ABI					
Product: 2tr	na310010b00	01_firmw	are		
Affected Vers	sion(s): * Up to	(excluding	g) 1.02		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/670
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System CVE ID: CVE-2024-4009	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/671
Product: 2tr	na310010b00	03_firmw	are		
Affected Vers	sion(s): * Up to	(excluding	g) 1.02		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/672
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bussystem CVE ID: CVE-2024-4009	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/673
	ma310011b00				
Affected Vers	sion(s): * Up to	(excludin		I	I
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/674
Authentica tion Bypass by	05-Jun-2024	7.8	Replay Attack	https://search.a bb.com/library/ Download.aspx?	O-ABB-2TMA- 200624/675
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Capture-replay In ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bussystem CVE ID: CVE-Z024-4009 Product: 2tma310011b0002_firmware Affected Version(s): * Up to (excluding) 1.02 FSDK Leak in ABB, Busch-Jaeger, FTS Display (version 1.3.0.33) allows attacker to take control via access to local KNX Buss-System UNauthoriz ed Actor Authentica tion Bypass by Capture-replay Authentica tion Bypass by Capture-replay CVE ID: CVE-Z024-4008 Authentica tion Bypass by Capture-replay CVE ID: CVE-Z024-4009 Authentica tion Bypass by Capture-replay CVE ID: CVE-Z024-4009 Product: 2tma310011b0003_firmware	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version (s): * Up to (excluding) 1.02 Exposure of Sensitive Informatio n to an Unauthoriz ed Actor Authentica tion Bypass by Capture-replay Capture-replay Authentica tion Bypass by Capture-replay CVE ID: ABB, Busch-Jaeger, FTS Display (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE-2024-4008 Replay Attack T.8 Authentica tion Bypass by Complete a co	_			Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX BusSystem CVE ID: CVE-	AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti	
Authentica tion Bypass by Capture-replay Ca	Product: 2ti	ma310011h00	02 firmw			
Exposure of Sensitive Informatio In to an Unauthoriz ed Actor Authentica tion Bypass by Capture-replay Authentica tion Bypass by Capture-replay CVE ID: CVE-toping (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System CVE ID: CVE-toping (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System O5-Jun-2024 7.8 Busch-Jaeger, FTS https://search.a bb.com/library/Download.aspx? DocumentID=9 AKK108464408 03&LanguageCo de=n&Docume ntPartId=&Acti On=Launch New York To Standard (version 1.00) and BCU (version 1.00) and BCU (version 1.00) and BCU (version 1.00) and BCU (version 1.30.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System CVE ID: CVE-toping						
Authentica tion Bypass by Capture-replay O5-Jun-2024 Capture-replay T.8 Authentica tion Bypass by Capture-replay Capture-replay CVE ID: CVE-2024-4009 CVE ID: CVE-2024-4009 In ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.30.33) allows attacker to Capture-replay (version 1.00) and BCU (version 1.30.33) allows attacker to Capture-replay (version 1.00) and BCU (version 1.30.33) allows attacker to Capture-replay (version 1.00) and BCU (version 1.30.33) allows attacker to Capture-replay (version 1.30.33) allows attacker (version 1.30.33) allows attacker (version	Exposure of Sensitive Informatio n to an Unauthoriz			FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE-	bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti	_
Product: 2tm2210011h0002 firmware	tion Bypass by Capture-	05-Jun-2024	7.8	in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System CVE ID: CVE-	bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti	
1 Toutet. Zillas Toot I Doods Ill ill wale	Product: 2ti	ma310011b00	03_firmw			

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to	excluding	g) 1.02		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	05-Jun-2024	8.8	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System CVE ID: CVE- 2024-4008	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/678
Authentica tion Bypass by Capture- replay	05-Jun-2024	7.8	in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System CVE ID: CVE-2024-4009	https://search.a bb.com/library/ Download.aspx? DocumentID=9 AKK108464A08 03&LanguageCo de=en&Docume ntPartId=&Acti on=Launch	O-ABB-2TMA- 200624/679
Vandarı Anı	nlo		2024-4009		
Vendor: App					
	sion(s): * Up to	(excluding	g) 12.5		
Out-of- bounds Write	10-Jun-2024	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted tiff file may lead to	https://support .apple.com/en- us/HT213345	O-APP-MACO- 200624/680

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
* stands for all versions					I	I		•		
			I	Page 398 d	of 471					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. CVE ID: CVE-		
Out-of- bounds Read	10-Jun-2024	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.5. Processing an AppleScript may result in unexpected termination or disclosure of process memory. CVE ID: CVE-2022-48578	https://support .apple.com/en- us/HT213345	O-APP-MACO- 200624/681
N/A	10-Jun-2024	5.3	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.5. A website may be able to track the websites a user visited in Safari private browsing mode. CVE ID: CVE-2022-32933	https://support .apple.com/en- us/HT213345	O-APP-MACO- 200624/682
Affected Ver	sion(s): * Up to	(excluding	g) 12.7.4		
N/A	10-Jun-2024	8.6	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5,	https://support .apple.com/en- us/HT214083, https://support .apple.com/en- us/HT214084, https://support	O-APP-MACO- 200624/683
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.7.4. An app may be able to break out of its sandbox. CVE ID: CVE- 2024-23299	.apple.com/en- us/HT214085	
N/A	10-Jun-2024	5.5	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data. CVE ID: CVE-	https://support .apple.com/en- us/HT214083, https://support .apple.com/en- us/HT214085	O-APP-MACO- 200624/684
Affected Ver	sion(s): * Up to	(excludin	2023-40389		
N/A	10-Jun-2024	7.8	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13. An app may be able to break out of its sandbox. CVE ID: CVE-2022-48683	https://support .apple.com/en- us/HT213488	O-APP-MACO- 200624/685
Affected Ver	sion(s): * Up to	(excludin	g) 14.4		
N/A	10-Jun-2024	5.5	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.4. An app may be	https://support .apple.com/en- us/HT214084	O-APP-MACO- 200624/686

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to access user- sensitive data. CVE ID: CVE- 2024-27792		
Affected Ver	 <mark>sion(s): From (i</mark>	ncluding)	13.0 Up to (excluding) 13.6.5	
N/A	10-Jun-2024	8.6	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to break out of its sandbox. CVE ID: CVE-2024-23299	https://support .apple.com/en- us/HT214083, https://support .apple.com/en- us/HT214084, https://support .apple.com/en- us/HT214085	O-APP-MACO- 200624/687
N/A	10-Jun-2024	5.5	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data. CVE ID: CVE-	https://support .apple.com/en- us/HT214083, https://support .apple.com/en- us/HT214085	O-APP-MACO- 200624/688
			2023-40389		
Affected Ver	sion(s): From (i	ncluding)	14.0 Up to (excluding) 14.4	
N/A	10-Jun-2024	8.6	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey	https://support .apple.com/en- us/HT214083, https://support .apple.com/en- us/HT214084, https://support	0-APP-MACO- 200624/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.7.4. An app may be able to break out of its sandbox.	.apple.com/en- us/HT214085	
			CVE ID: CVE- 2024-23299		
Vendor: Can	onical				
Product: ub	untu_linux				
Affected Vers	sion(s): 18.04				
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot CVE ID: CVE-2022-28657	N/A	O-CAN-UBUN- 200624/690
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections CVE ID: CVE- 2022-28655	N/A	O-CAN-UBUN- 200624/691
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	04-Jun-2024	5.5	~/.config/apport/s ettings parsing is vulnerable to "billion laughs" attack CVE ID: CVE- 2022-28652	N/A	0-CAN-UBUN- 200624/692
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log CVE ID: CVE- 2022-28654	N/A	0-CAN-UBUN- 200624/693
Allocation of	04-Jun-2024	5.5	is_closing_session() allows users to	N/A	0-CAN-UBUN- 200624/694
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 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			consume RAM in the Apport process CVE ID: CVE- 2022-28656			
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing CVE ID: CVE-2022-28658	N/A	O-CAN-UBUN- 200624/695	
Affected Vers	sion(s): 20.04					
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot CVE ID: CVE-2022-28657	N/A	O-CAN-UBUN- 200624/696	
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections CVE ID: CVE- 2022-28655	N/A	O-CAN-UBUN- 200624/697	
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	04-Jun-2024	5.5	~/.config/apport/s ettings parsing is vulnerable to "billion laughs" attack CVE ID: CVE- 2022-28652	N/A	O-CAN-UBUN- 200624/698	
Allocation of Resources Without CVSSv3 Scoring	04-Jun-2024 Scale 0-1	5.5	is_closing_session() allows users to fill up apport.log	N/A 5-6 6-7 7-8	O-CAN-UBUN- 200624/699	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			CVE ID: CVE- 2022-28654		
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process CVE ID: CVE- 2022-28656	N/A	O-CAN-UBUN- 200624/700
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing CVE ID: CVE-	N/A	O-CAN-UBUN- 200624/701
A CC . LY	. () 24.40		2022-28658		
Affected Ver	sion(s): 21.10				I
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot CVE ID: CVE-2022-28657	N/A	O-CAN-UBUN- 200624/702
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections CVE ID: CVE- 2022-28655	N/A	O-CAN-UBUN- 200624/703
Improper Restriction of Recursive Entity References in DTDs ('XML Entity	04-Jun-2024	5.5	~/.config/apport/s ettings parsing is vulnerable to "billion laughs" attack CVE ID: CVE- 2022-28652	N/A	O-CAN-UBUN- 200624/704

CVSSv3 Scoring Scale	0-1	1-2	2-3	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'					
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log CVE ID: CVE- 2022-28654	N/A	O-CAN-UBUN- 200624/705
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process CVE ID: CVE- 2022-28656	N/A	O-CAN-UBUN- 200624/706
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing CVE ID: CVE-2022-28658	N/A	O-CAN-UBUN- 200624/707
Affected Ver	sion(s): 22.04			l	I
N/A	04-Jun-2024	7.8	Apport does not disable python crash handler before entering chroot CVE ID: CVE-2022-28657	N/A	O-CAN-UBUN- 200624/708
Allocation of Resources Without Limits or Throttling	04-Jun-2024	7.1	is_closing_session() allows users to create arbitrary tcp dbus connections CVE ID: CVE- 2022-28655	N/A	O-CAN-UBUN- 200624/709
Improper Restriction of Recursive	04-Jun-2024	5.5	~/.config/apport/s ettings parsing is vulnerable to	N/A	O-CAN-UBUN- 200624/710

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Entity References in DTDs ('XML Entity Expansion')			"billion laughs" attack CVE ID: CVE- 2022-28652	attack CVE ID: CVE-			
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to fill up apport.log CVE ID: CVE- 2022-28654	allows users to fill up apport.log N/A CVE ID: CVE-			
Allocation of Resources Without Limits or Throttling	04-Jun-2024	5.5	is_closing_session() allows users to consume RAM in the Apport process CVE ID: CVE- 2022-28656	N/A	O-CAN-UBUN- 200624/712		
N/A	04-Jun-2024	5.5	Apport argument parsing mishandles filename splitting on older kernels resulting in argument spoofing CVE ID: CVE-2022-28658	ort argument ing mishandles ame splitting older kernels Iting in ment spoofing ID: CVE-			
Vendor: Del	bian						
Product: de	bian_linux						
Affected Ver	sion(s): 10.0						
Out-of- bounds Read	05-Jun-2024	8.1	An out-of-bounds read in the 'bson' module of PyMongo 4.6.2 or earlier allows deserialization of malformed BSON provided by a Server to raise an exception which may contain	https://jira.mo ngodb.org/bro wse/PYTHON- 4305	O-DEB-DEBI- 200624/714		
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-	8 8-9 9-10		

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary application memory.		
			CVE ID: CVE- 2024-5629		
Vendor: Fed	loraproject				
Product: fed	lora				
Affected Vers	sion(s): 40				
Improper Encoding or Escaping of Output	09-Jun-2024	8.8	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell. CVE ID: CVE-2024-5585	N/A	O-FED-FEDO- 200624/715
Observable Discrepanc y	09-Jun-2024	5.9	The openssl_private_de crypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_	N/A	O-FED-FEDO- 200624/716

CVSSv3 Scoring Scale 0-1
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PADDING, which is the default), is		
			vulnerable to the Marvin Attack		
			unless it is used		
			with an OpenSSL		
			version that		
			includes the		
			changes from this		
			pull request:		
			https://github.com /openssl/openssl/		
			pull/13817		
			(rsa_pkcs1_implicit		
			_rejection). These		
			changes are part of		
			OpenSSL 3.2 and		
			have also been		
			backported to stable versions of		
			various Linux		
			distributions, as		
			well as to the PHP		
			builds provided for		
			Windows since the		
			previous release.		
			All distributors and		
			builders should ensure that this		
			version is used to		
			prevent PHP from		
			being vulnerable.		
			_		
			PHP Windows		
			builds for the		
			versions 8.1.29, 8.2		
			.20 and 8.3.8 and		
			above include		
			OpenSSL patches		
			that fix the		
			vulnerability.		
			CVE ID: CVE-		
			2024-2408		
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verificatio n of Data Authenticit y	09-Jun-2024	5.3	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VAL IDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly. CVE ID: CVE-2024-5458	https://github.c om/php/php- src/security/ad visories/GHSA- w8qr-v226- r27w	O-FED-FEDO- 200624/717
Vendor: Goo	ogle				
Product: an	droid				
Affected Ver	sion(s): -				
N/A	13-Jun-2024	7.8	there is a possible way to bypass 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	https://source.a ndroid.com/sec urity/bulletin/p ixel/2024-06- 01	0-G00-ANDR- 200624/718

CVSSv3 Scoring Scale
* stands for all versions

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation. CVE ID: CVE-2024-32896		
Vendor: IBN	<u> </u> 				
Product: i					
Affected Ver	sion(s): 7.2				
Observable Discrepanc y	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538. CVE ID: CVE-2024-31878	https://exchang e.xforce.ibmclou d.com/vulnerab ilities/287538, https://www.ib m.com/support /pages/node/7 156725	O-IBM-I- 200624/719
Affected Ver	sion(s): 7.3				
Observable Discrepanc y	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks.	https://exchang e.xforce.ibmclou d.com/vulnerab ilities/287538, https://www.ib m.com/support /pages/node/7 156725	O-IBM-I- 200624/720

CVSSv3 Scoring Scale	0-1	1-2	2-3	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: 287538. CVE ID: CVE-2024-31878		
Affected Ver	sion(s): 7.4				
Observable Discrepanc y	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538. CVE ID: CVE-2024-31878	https://exchang e.xforce.ibmclou d.com/vulnerab ilities/287538, https://www.ib m.com/support /pages/node/7 156725	O-IBM-I- 200624/721
Affected Ver	sion(s): 7.5				
Observable Discrepanc y	07-Jun-2024	5.3	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538.	https://exchang e.xforce.ibmclou d.com/vulnerab ilities/287538, https://www.ib m.com/support /pages/node/7 156725	O-IBM-I- 200624/722

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID: CVE- 2024-31878					
Vendor: Linux								
Product: lin								
Affected Ver	sion(s): 6.10.0		I					
			In the Linux kernel, the following vulnerability has been resolved:					
			net: fixdst_negative_advi ce() race					
		dst_negative_advi ce() does not enforce proper RCU rules when						
			sk->dst_cache must be cleared, leading to possible UAF.	el.org/stable/c/ 92f1655aa2b22 94d0b49925f3b 875a634bd3b5 9e, https://git.kern el.org/stable/c/ b8af8e6118a66				
Use After	10-Jun-2024	7.8	RCU rules are that we must first clear sk->sk_dst_cache,		0-LIN-LINU-			
Free			then call dst_release(old_dst).		200624/723			
		Note that sk_dst_reset(sk) is implementing this protocol correctly,	C 210344034301					
		whiledst_negative_advi ce() uses the wrong order.						
			Given that ip6_negative_advic e() has special logic					
			against RTF_CACHE, this means each of the					

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			three - >negative_advice()		
			existing methods must perform the sk_dst_reset() themselves.		
			Note the check against NULL dst is centralized in		
			dst_negative_advi ce(), there is no need to duplicate		
			it in various callbacks.		
			Many thanks to Clement Lecigne for tracking this issue.		
			This old bug became visible after the blamed commit, using UDP sockets.		
			CVE ID: CVE- 2024-36971		
Affected Vers	sion(s): From (i	ncluding)	4.6 Up to (excluding)	6.9.4	
			In the Linux kernel, the following vulnerability has been resolved:	https://git.kern el.org/stable/c/ 92f1655aa2b22 94d0b49925f3b	
Use After Free	10-Jun-2024	7.8	net: fix dst_negative_advi ce() race	875a634bd3b5 9e, https://git.kern el.org/stable/c/ b8af8e6118a66	O-LIN-LINU- 200624/724
			dst_negative_advi ce() does not enforce proper RCU rules when	05f0e495a58d5 91ca94a85a50f c	

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk->dst_cache must be cleared, leading to possible UAF.		
			RCU rules are that we must first clear sk->sk_dst_cache,		
			then call dst_release(old_dst).		
			Note that sk_dst_reset(sk) is implementing this protocol correctly, whiledst_negative_advice() uses the wrong order.		
			Given that ip6_negative_advic e() has special logic		
			against RTF_CACHE, this means each of the three - >negative_advice()		
			existing methods must perform the sk_dst_reset() themselves.		
			Note the check against NULL dst is centralized in		
			dst_negative_advi ce(), there is no need to duplicate		

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it in various callbacks.		
			Many thanks to Clement Lecigne for tracking this issue.		
			This old bug became visible after the blamed commit, using UDP sockets.		
			CVE ID: CVE- 2024-36971		
Vendor: Mic					
Product: wi					
Affected Ver	sion(s): -				T
Improper Link Resolution Before File Access ('Link Following')	10-Jun-2024	7	A sym-linked file accessed via the repair function in Avast Antivirus <24.2 on Windows may allow user to elevate privilege to delete arbitrary files or run processes as NT AUTHORITY\SYST EM. The vulnerability exists within the "Repair" (settings -> troubleshooting -> repair) feature, which attempts to delete a file in the current user's AppData directory as NT AUTHORITY\SYST	N/A	O-MIC-WIND- 200624/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EM. A low-privileged user can make a pseudo-symlink and a junction folder and point to a file on the system. This can provide a low-privileged user an Elevation of Privilege to win a race-condition which will recreate the system files and make Windows callback to a specially-crafted file which could be used to launch a privileged shell instance. This issue affects Avast Antivirus prior to 24.2. CVE ID: CVE-2024-5102		
Product: wi	ndows_10_150	7			
Affected Ver	sion(s): * Up to	(excludin	g) 10.0.10240.20680		
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/726
Product: wi	ndows_10_160	7			
Affected Ver	sion(s): * Up to	(excludin	g) 10.0.14393.7070		
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code	https://msrc.mi crosoft.com/up date-	O-MIC-WIND- 200624/727
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability CVE ID: CVE- 2024-30080	guide/vulnerabi lity/CVE-2024- 30080	
Product: wi	ndows_10_180	9			l
Affected Ver	sion(s): * Up to	(excludin	g) 10.0.17763.5936		
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/728
Product: wi	ndows_10_21h	1			
Affected Ver	sion(s): * Up to	(excludin	g) 10.0.19043.4529		
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/729
Product: wi	ndows_11_21h	2			
Affected Ver	sion(s): * Up to	(excludin	g) 10.0.22000.3019		
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/730
Product: wi	ndows_11_22h	2			
Affected Ver	sion(s): * Up to	(excludin	g) 10.0.22621.3737		
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	https://msrc.mi crosoft.com/up date- guide/vulnerabi	O-MIC-WIND- 200624/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID: CVE- 2024-30080	lity/CVE-2024- 30080					
Product: windows_11_23h2									
Affected Ver	sion(s): * Up to	(excluding	g) 10.0.22631.3737						
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/732				
Product: wi	ndows_server_	2008							
Affected Ver	sion(s): -								
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/733				
Affected Ver	sion(s): r2			I	I				
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE-	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/734				
D 1	•	2042	2024-30080						
	ndows_server_	2012							
Affected Ver	sion(s): -		Migrogoft Massac						
Use After Free	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/735				
Affected Ver	sion(s): r2								
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8					

Wea	kness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Use Free	After	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/736				
Prod	Product: windows_server_2016									
Affect	ted Vers	sion(s): -								
Use Free	After	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/737				
Prod	uct: wi	ndows_server_	2019			l				
Affect	ted Vers	sion(s): * Up to	(excluding	g) 10.0.17763.5936						
Use Free	After	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/738				
Prod	uct: wi	ndows_server_	2022			1				
Affect	ted Vers	sion(s): * Up to	(excluding	g) 10.0.20348.2522						
Use Free	After	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	https://msrc.mi crosoft.com/up date- guide/vulnerabi lity/CVE-2024- 30080	O-MIC-WIND- 200624/739				
Prod	uct: wi	ndows_server_	2022_23	h2						
Affect	ted Vers	sion(s): * Up to	(excluding	g) 10.0.25398.950						
Use Free	After	11-Jun-2024	9.8	Microsoft Message Queuing (MSMQ)	https://msrc.mi crosoft.com/up	O-MIC-WIND- 200624/740				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability CVE ID: CVE- 2024-30080	date- guide/vulnerabi lity/CVE-2024- 30080	
Vendor: Mit	el				1
Product: 68	69i_sip_firmw	are			
Affected Ver	sion(s): * Up to	(including	g) 4.5.0.41		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-Jun-2024	8.8	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in	N/A	O-MIT-6869- 200624/741

CVSSv3 Scoring Scale	0-1	1-2	2-3	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 hostname parameter. CVE ID: CVE-2024-37569		
Affected Vers	sion(s): 4.5.0.41				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-Jun-2024	8.8	On Mitel 6869i 4.5.0.41 devices, the Manual Firmware Update (upgrade.html) page does not perform sanitization on the username and path parameters (sent by an authenticated user) before appending flags to the busybox ftpget command. This leads to \$() command execution. CVE ID: CVE- 2024-37570	N/A	O-MIT-6869- 200624/742
Affected Ver	sion(s): From (i	ncluding)	5.0.0.0 Up to (includi	ng) 5.0.0.1018	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-Jun-2024	8.8	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname	N/A	O-MIT-6869- 200624/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in the hostname parameter. CVE ID: CVE-		
			2024-37569		
Vendor: Red					
	terprise_linux				
Affected Ver	sion(s): 7.0				
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/744
Affected Ver	sion(s): 8.0				<u> </u>
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/745
n of Data CVSSv3 Scoring * stands for all years		1-2 2		5-6 6-7 7-8	,

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049							
Affected Ver	Affected Version(s): 9.0									
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/746					
Product: en	terprise_linux	_eus								
Affected Ver	sion(s): 8.4									
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/747					
Affected Ver	sion(s): 8.8									
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/748					

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-				
			2024-3049				
Affected Vers	sion(s): 9.2						
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/749		
Product: en	terprise_linux	_for_arm_	64				
Affected Vers	sion(s): 8.0_aar	ch64					
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/750		
Affected Version(s): 8.8_aarch64							
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/751		

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049				
Affected Vers	sion(s): 9.2_aar	ch64					
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/752		
Affected Vers	sion(s): 9.4_aar	ch64		L			
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/753		
Product: en	terprise_linux_	for_ibm_					
	Affected Version(s): 8.0_s390x						
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/754		

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049		
Affected Vers	sion(s): 9.2_s39	0x			
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/755
Affected Vers	sion(s): 9.4_s39	0x			
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/756
Product: en	terprise_linux_	_for_ibm_	z_systems_eus		
Affected Vers	sion(s): 8.8_s39	0x			
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/757

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049		
Product: en	terprise_linux	_for_pow	er_little_endian_eus		
Affected Ver	sion(s): 8.0_ppc	:64le			
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server.	N/A	O-RED-ENTE- 200624/758
			CVE ID: CVE- 2024-3049		
Affected Ver	sion(s): 8.4_ppc	:64le			
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/759
Affected Ver	sion(s): 8.8_ppc	:64le			
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/760

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server.		
			CVE ID: CVE- 2024-3049		
Affected Vers	sion(s): 9.2_ppc	64le			
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049	N/A	O-RED-ENTE- 200624/761
Affected Ver	sion(s): 9.4_ppc	64le	1	l	l
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-	N/A	O-RED-ENTE- 200624/762
			2024-3049		
	•	_server_u	pdate_services_for_s	ap_solutions	
Affected Ver	sion(s): 8.4				I
Insufficient Verificatio n of Data	06-Jun-2024	5.9	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted	N/A	O-RED-ENTE- 200624/763

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticit y			hash is passed to gcry_md_get_algo_d len(), it may allow an invalid HMAC to be accepted by the Booth server. CVE ID: CVE-2024-3049		
Vendor: San	nsung				
Product: exy	ynos_1080_firr	nware			
Affected Vers	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/764

CVSSv3 Scoring Scale	0.1	1.2	2.2	2.4	4 F	ГС	6.7	7.0	0.0	0.10
L CVSSV3 SCOTING SCALE	()- (l I-/	7-3	3-4	4-5) - D	n-/	I /-X	X-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/765
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/766

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE II	D Patch	NCIIPC ID
			Modem 5300, an Exynos Aut T5123. The baseband softwar does not proper check format type specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE 2023-49927	e e e y es e e d d of	
N/A	05-Jun-2024	5.3	An issue wadiscovered is Samsung Mobil Processor, Automotive Processor, and Modem Exynology (1982), 9825, 986, 990, 850, 1086, 2100, 2200, 1286, 1380, 1330, Modem 5123, Modem 5300, and Auto T512. The baseband software does not properly check replay protection specified by the NAS (Non-Access Stratum) modul This can lead to denial of service. CVE ID: CVE 2023-50803	d d d d d d d d d d d d d d d d d d d	0-SAM-EXYN-
	ynos_1280_firi	nware			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue wa discovered i Samsung Mobil Processor,	n ductor.samsung	O-SAM-EXYN-
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7	-8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE- 2024-29152	support/produc t-security- updates/	
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/769

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description &	CVE ID		Patch		NCIIP	C ID
			baseband so does not procheck specified be RRC. This can be a consistive information. CVE ID: 2023-49928	states y the an lead are of					
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	Processor, Automotive Processor, Wearable Processor, Modem 980, 990, 1080, 2100, 1280, 1380, 9110, Exynos	2200, 1330, W920, Modem Exynos 0, and Auto The oftware coperly t types y the an lead ck of	ducto .com, uality	ort/pro urity-	ung t/q	0-SAM-E 200624/	
N/A	05-Jun-2024	5.3	An issue discovered Samsung Processor, Automotive Processor,	was in Mobile and	ducto .com, uality	://semi or.samsu /suppor ort/pro	ung t/q	0-SAM-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Modem Exynos 9820, 9825, 982 990, 885, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5123, Modem 5123, Modem 5123, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803 CVE-2023-50803	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: exyus_1330_fir=ware Affected Versus_sis_sis_sis_us_a discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration Product: exyus_sis_1330_fir=ware_sis_1330_fir				9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to	_	
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung Mobile Processor, and https://semicon ductor.samsung.com/support/q uality-support/produc t-security-updates/						
N/A O4-Jun-2024 7.5 An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 980, 990, 850, ductor.samsung .com/support/q uality-uality-updates/ O-SAM-EXYN-200624/772			nware			
M/A O4-Jun-2024 7.5 discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5123, Modem 5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, will rescurity updates/ O-SAM-EXYN-200624/772	Affected Ver	sion(s): -		An issue was		
				discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration	ductor.samsung .com/support/q uality- support/produc t-security- updates/	200624/772

^{*} stands for all versions

			_								CID
			le se in C '	essage. The state of the state	closure of n. CVE-						
N/A C	05-Jun-2024	7.5	Sa Pri AA Pri W Pri M 98 10 12 92 55 M Ex Th ba do ch see in C	scovered amsung rocessor, utomotive rocessor, dearable rocessor, odem 80, 990 280, 138 110, synos 123, odem 53 synos 5123. Asseband pes not neck pecified RC. This odisclosensitive aformation VE ID:	in Mobile e and Exynos 0, 850, 0, 2200, 0, 1330, W920, Modem Exynos 800, and Auto The software properly states by the can lead sure of n. CVE-	http: duct .com ualit supp t-sec upda	s://semi or.sams i/suppor y- port/pro curity- ates/	ung t/q	O-SAI 2006		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	Ai di Sa Pi A Pi W	n issued scovered amsung rocessor, utomotive rocessor, vearable rocessor,	e was in Mobile	duct .com ualit supp t-sec	s://semi or.sams i/suppor y- port/pro curity- ates/	ung t/q	0-SAI 2006		
CVSSv3 Scoring Sco	ale 0-1	1-2		odem 3-4	Exynos 4-5	5-6	6-7	7-8		-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/775

CVSSv3 Scoring Scale
* stands for all versions 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ynos_1380_firm	nware			
rsion(s): -				
04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/776
05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/777
	04-Jun-2024	04-Jun-2024 7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1080, 2100, 2200,	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Wearable Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, wighted the processor of the security-updates/

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/778

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/779
	ynos_2100_firi	nware			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/780
CVSSv3 Scoring	Scale 0-1	1-2 2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	3	Description	& CVE ID		Patch		NCIIP	CID
				software or properly states speche RRC Resource Reconfigurates age. ead to disconsitive information CVE ID: 2024-291	check cified by (Radio Control) ration This can closure of n. CVE-					
N/A	05-Jun-2024	7.5		An issudiscovered Samsung Processor, Automotive Processor, Wearable Processor, Modem 980, 990, 1280, 138, 138, 138, 138, 138, 138, 138, 138	e and Exynos 0, 850, 00, 2200, W920, Modem Exynos 300, and Auto The software properly states by the can lead sure of n.	htt duo .co ual sup t-so upo	ps://semetor.sams m/suppo ity- pport/pre ecurity- dates/	sung ort/q	O-SAM-E 200624/	
Missing Encryption	05-Jun-2024	5.3		An issu discovered Samsung		du	ps://sem ctor.sams m/suppo	sung	O-SAM-E 200624/	
CVSSv3 Scoring	Scale 0-1	1-2	2-3		4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE- 2023-49927	uality- support/produc t-security- updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	0-SAM-EXYN- 200624/783

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ev	ynos_2200_firr	nwaro	Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803		
Affected Ver		- Inware			
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/784
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor,	https://semicon ductor.samsung .com/support/q uality- support/produc	O-SAM-EXYN- 200624/785
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE- 2023-49928	t-security- updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/786

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/787
Product: ex	ynos_2400_firi	nware			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/788
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1080, 2100, 2200, 1280, 1380, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information.		
Product: ex	ynos_850_firm	ware	CVE ID: CVE- 2024-29152		
Affected Ver					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control)	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/789
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE-2023-49928	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/790
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/791

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A CVSSv3 Scoring	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN-200624/792

CVSSv3 Scoring Scale
* stands for all versions

Product: ex Affected Ver	ynos_9110_fir rsion(s): -	nware			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/793
Product: ex	ynos_980_firm	ware			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152		
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/795

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		to disclosure of sensitive information. CVE ID: CVE-2023-49928		
05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/796
05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	0-SAM-EXYN- 200624/797
	05-Jun-2024	05-Jun-2024 5.3	to disclosure of sensitive information. CVE ID: CVE-2023-49928 An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5300, and Exynos Auto T5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, Automotive Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280,	to disclosure of sensitive information. CVE ID: CVE-2023-49928 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5123, Exynos Modem 5123, Exynos Modem 5123, The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 9820, 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, and Exynos 9820, 9

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.		
			CVE ID: CVE- 2023-50803		
	ynos_9820_firi	nware			
Affected Ver	sion(s): -				
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/798

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE- 2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/799
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/800

CVSSv3 Scoring Scale
* stands for all versions

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software does not properly check replay protection specified by the NAS (Non-Access Stratum) module This can lead to denial of service. CVE ID: CVE		
Product: ex	ynos_9825_firi	nware	2023-50803		
Affected Ver		invare			
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850 1080, 2100, 2200 1280, 1380, 1330 9110, W920 Exynos Modem 5300, and Exynos Automotive T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE 2023-49928	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/801
Missing Encryption	05-Jun-2024	5.3	An issue was discovered ir	1 , ,	O-SAM-EXYN- 200624/802
CVSSv3 Scoring	Scale 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-	8 8-9 9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	.com/support/q uality- support/produc t-security- updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/803

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803		
Product: ex	ynos_990_firm	ware			
Affected Ver	sion(s): -				
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/804
N/A	05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive	https://semicon ductor.samsung .com/support/q uality- support/produc	O-SAM-EXYN- 200624/805

CVSSv3 Scoring Scale
* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information. CVE ID: CVE- 2023-49928	t-security- updates/	
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/806

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927		
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/807
	ynos_auto_t51	23_firmw	are		
Affected Vers	Sion(s): -		An iccuo was		
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/808
CVSSv3 Scoring	Scale 0-1	1-2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

^{*} stands for all versions

980, 990, 850, 1080, 2100, 2200, 1280, 1330, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE_2024-29152	Weakness	Publish Date	CVSSv3	Description	& CVE ID	Patch		NCIIP	C ID
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, Expnos 980, 990, 850, 1280, 1380, 1330, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5123, Modem 5123, Modem 5123. The baseband software does not properly check states specified by				1080, 2100 1280, 1380 2400, 9110 W930, 5123, Mode and Auto The b software d properly states spec the RRC Resource Reconfigura message. T lead to discl sensitive information CVE ID:	0, 2200, 0, 1330, 0, W920, Modem em 5300, T5123. aseband loes not check cified by (Radio Control) ation This can losure of the CVE-				
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by An issue was discovered in Samsung whobile Processor, Automotive Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 13	D 1 .	•	1400 C		52				
An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by			5123_firn	iware					
discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by	Affected Ver	sion(s): -						T	
	N/A	04-Jun-2024	7.5	discovered Samsung Processor, Wearable Processor, Automotive Processor, Modem 980, 990 1080, 2100 1280, 1380 2400, 9110 W930, 5123, Mode and Auto The b software d properly states spec	in Mobile and Exynos by 850, conductive years conductive	ductor.samsung .com/support/q uality- support/produc t-security-			

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Des	Description & CVE ID			Patch			NCIIPC ID	
		Red med lead sen info	Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE- 2024-29152								
N/A	05-Jun-2024	7.5	San Pro Aut Pro We Pro Mo 980 108 128 911 Exy 512 Mo Exy T52 bas doe che spe RRO to sen info	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead			s://sem or.sams i/suppor y- oort/pro curity- ates/	ung rt/q	O-SAM-EXYN- 200624/810		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An disc San Pro	An issue was discovered in Samsung Mobile Processor, Automotive Processor,			s://sem or.sams /suppor y- oort/pro	ung rt/q	O-SAM-EXYN- 200624/811		
CVSSv3 Scoring	Scale 0-1	1-2	We	arable 3-4	4-5	5-6	6-7	7-8	8-9	9-10	

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption. CVE ID: CVE-2023-49927	t-security- updates/	
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/812

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

		CVE ID: CVE- 2023-50803		
kynos_modem_5	5300_firn	ıware		
rsion(s): -				
04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/813
05-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/814
	04-Jun-2024	04-Jun-2024 7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-2024-29152 An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Unity-support/quality-support/product-security-updates/

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.		
			CVE ID: CVE- 2023-49928		
Missing Encryption of Sensitive Data	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. The baseband software does not properly check format types specified by the RRC. This can lead	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/815

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			to a lack of encryption. CVE ID: CVE-2023-49927			
N/A	05-Jun-2024	5.3	An issue was discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service. CVE ID: CVE-2023-50803	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/816	
Product: exy	ynos_w920_fir	mware				
Affected Vers	sion(s): -					
N/A	04-Jun-2024	7.5	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330,	https://semicon ductor.samsung .com/support/q uality- support/produc t-security- updates/	O-SAM-EXYN- 200624/817	
CVSSv3 Scoring	Scale 0-1	1-2 2	-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10	
* stands for all ve						

An issue was discovered in Samsung Mobile Processor, Automotive	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): - An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration An issue was discovered in Samsung Mobile Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, w930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration	Droduct: av	vnoc w020 fin	mwara	W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration message. This can lead to disclosure of sensitive information. CVE ID: CVE-				
N/A O4-Jun-2024 7.5 discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration discovered in Samsung Mobile Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control) Reconfiguration			in war c					
messager rms carr			7.5	discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 2200, 1280, 1380, 1330, 2400, 9110, W920, W930, Modem 5123, Modem 5300, and Auto T5123. The baseband software does not properly check states specified by the RRC (Radio Resource Control)	ductor.samsung .com/support/q uality- support/produc t-security-			

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to disclosure of sensitive information. CVE ID: CVE-2024-29152		
Vendor: Te	ndacn				
Product: o3	v2_firmware				
Affected Ver	sion(s): 1.0.0.12	2\\(3880\	(/)		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	04-Jun-2024	9.8	Tenda 03V2 v1.0.0.12(3880) was discovered to contain a Blind Command Injection via stpEn parameter in the SetStp function. This vulnerability allows attackers to execute arbitrary commands with root privileges. CVE ID: CVE- 2024-36604	N/A	O-TEN-03V2- 200624/819
Vendor: un	iview				
Product: nv	r301-04s2-p4	firmwar	9		
Affected Ver	sion(s): * Up to	(excluding	g) nvr-b3801.20.17.24	10507	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-Jun-2024	5.4	Uniview NVR301- 04S2-P4 is vulnerable to reflected cross-site scripting attack (XSS). An attacker could send a user a URL that if clicked on could execute malicious JavaScript in their browser. This vulnerability also requires	N/A	O-UNI-NVR3- 200624/820

CVSSv3 Scoring Scale 0-1 1	1-2 2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
----------------------------	---------	---------	-----	-----	-----	-----	------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication before it can be exploited, so the scope and severity is limited. Also, even if JavaScript is executed, no additional benefits are obtained. CVE ID: CVE- 2024-3850		
Vendor: vw					
	charger_conne	ct_firmw	are		
Affected Ver	sion(s): spr3.2				
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass	N/A	0-VW-ID.C- 200624/821

CVSSv3 Scoring Scale
* stands for all versions

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. CVE ID: CVE-2024-5684		
Affected Ver	sion(s): spr3.51				
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit	N/A	O-VW-ID.C- 200624/822

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

3-4

this vulnerability to bypass the authentication mechanism. CVE ID: CVE-2024-5684 Affected Version(s): spr3.52 An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is swrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism.	Weakness	Publish Date	CVSSv3	Description &	CVE ID	Patch	NCIIP	C ID
An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none" algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication	Affected Ver	sion(s)· snr3 52		bypass authentication mechanism. CVE ID:	the			
Insufficient Verificatio n of Data Authenticit y 06-Jun-2024 8.8 8.8 06-Jun-2024 Authenticit y 08-Jun-2024 Authenticit y 8.8 8.8 8.8 8.8 8.8 8.8 8.8								
CVSSv3 Scoring Scale	Verificatio n of Data Authenticit y			private ne (the charg connected local access Ethernet-Internet can exploit a implementate the JWT-librorder to byp password authentication the configuration interface an has full accept have. However attacker with the JWT-librorder to accept have develor admin rights implementate the JWT-librorder will insecure will insecu	etwork ger is to) or to the erface a faulty cion of cary in ass the on to web and then cess as would ver, an ill not oper or s. If the cion of crary is figured 'none"- the pass WT. A ated exploit bility to the on		200624/	823

^{*} stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID: CVE- 2024-5684					
Product: id.charger_pro_firmware								
Affected Ver	sion(s): spr3.2							
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. CVE ID: CVE-2024-5684	N/A	O-VW-ID.C- 200624/824			

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): spr3.51				
Insufficient Verificatio n of Data Authenticit y	06-Jun-2024	8.8	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism. CVE ID: CVE-2024-5684	N/A	O-VW-ID.C- 200624/825
Affected Vers	sion(s): spr3.52		An attacker with		O MAY ID C
Verificatio n of Data CVSSv3 Scoring	06-Jun-2024 Scale 0-1	1-2 2	access to the private network	N/A 5-6 6-7 7-	0-VW-ID.C- 200624/826 8 8-9 9-10

^{*} stands for all versions

Authenticit y (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the	NCIIPC ID	Patch	Description & CVE ID	CVSSv3	Publish Date	Weakness
local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			(the charger is			Authenticit
Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			connected to) or			y
can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			local access to the			
implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			Ethernet-Interface			
implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			can exploit a faulty			
the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			_			
password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			•			
authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			-			
configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			_			
the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			_			
the JWT-library is wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
wrongly configured to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			_			
to accept "none"- algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			-			
algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to						
insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to			_			
local, unauthenticated attacker can exploit this vulnerability to			-			
unauthenticated attacker can exploit this vulnerability to			ŕ			
attacker can exploit this vulnerability to			·			
this vulnerability to						
bypass the			_			
authentication						
mechanism.			mechanism.			
CVE ID: CVE-			CVE ID: CVE-			
2024-5684						

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	