https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 28 Feb 2025 Vol. 12 No. 04

Table of Content

Vendor	Product	Page Number
Application		
1clickmigration	1_click_migration	1
adityapatadia	gumlet_video	1
akashmalik	scracth_\&_win	2
amauri	wpmobile.app	2
amothemo	amo_team_showcase	3
backie	option_editor	3
bandsintown	bandsintown	4
benbodhi	svg_support	4
better-auth	better_auth	5
bigbuy	dropshipping_connector_for_woocommerce	6
bishopfox	sliver	6
byconsole	wooodt_lite	7
carspot_project	carspot	7
catsone	cats_job_listings	8
churchcrm	churchcrm	8
Cisco	openh264	12
clavaque	s2member	14
cmseasy	cmseasy	14
CMU	ghosts	15
code-projects	blood_bank_system	16
codemenschen	gift_vouchers	16
Combodo	itop	17
covertnine	c9_admin_dashboard	17
	c9_blocks	18
cyberchimps	responsive_addons_for_elementor	18
dcurasi	cookie_notice_bar	19

Vendor	Product	Page Number
debounce	email_validator	19
elementor	website_builder	20
eniture	ltl_freight_quotes	20
	small_package_quotes	23
ex-themes	woocommerce_food	25
fabianros	real_estate_property_management_system	25
formassembly	wp-formassembly	26
Genetechsolutions	pie_register	26
Glpi-project	glpi	27
goodlayers	tour_master	28
haozhexie	wp-bibtex	28
homeasap	easy_mls_listings_import	29
icopydoc	maps_for_wp	29
igumbi	igumbi	30
imaginate-solutions	file_uploads_addon_for_woocommerce	30
imamura	newpost_catch	30
iptanus	wordpress_file_upload	31
istmoplugins	get_bookings_wp	31
jakob42	reaction_buttons	32
janobe	e-learning_system	33
jonathanjernigan	pie_calendar	33
keap	keap_official_opt_in_forms	34
kerryoco	threepress	34
kevinbrent	wprequal	35
Kriesi	enfold	35
legoeso	pdf_manager	36
lightspeedhq	ecwid_ecommerce_shopping_cart	37
lmxcms	lmxcms	37
localsend	localsend	38
magayo	magayo_lottery_results	38
magazine3	web_stories_enhancer	39
marcoingraiti	actionwear_products_sync	39

Vendor	Product	Page Number
matiskiba	ravpage	40
mayurik	best_church_management_software	41
	best_employee_management_system	42
megaoptim	rapid_cache	43
metabase	metabase	43
metagauss	profilegrid	47
Microsoft	power_pages	48
minicoursegenerator	mini_course_generator	48
mlcalc	mortgage_loan_calculator	49
modalsurvey	simple_signup_form	49
modernasistemas	modernanet	50
monospace	directus	52
mrlegend1235	typed_js	54
navidrome	navidrome	54
Ncrafts	formcraft	55
needyamin	library_card_system	56
nilambar	prime_addons_for_elementor	57
Odoo	odoo	57
oliverfriedmann	ziggeo	58
patternsinthecloud	autoship_cloud	58
photonicgnostic	library_bookshelves	59
phpgurukul	online_nurse_hiring_system	59
	online_shopping_portal	60
Phusion	passenger	61
pinpoint	pinpoint_booking_system	61
pixelgrade	open_hours	62
pixelite	events_manager	62
platcom	wp-asambleas	63
pluginus	active_products_tables_for_woocommerce	63
presslayouts	pressmart	64
radiustheme	classified_listing	64
raptive	raptive_ads	65

Vendor	Product	Page Number
razormist	employee_management_system	66
royal-elementor-addons	royal_elementor_addons	66
ryansolid	dom_expressions	66
satollo	head\,_footer\,_and_post_injections	68
seacms	seacms	68
shaonback2	simple_map_no_api	68
shenyanzhi	memorialday	69
shopwarden	shopwarden	69
simplebooklet	simplebooklet	70
smartzminds	reset	70
softdiscover	zigaform	71
speedsize	speedsize_image_\&_video_ai-optimizer	72
supporthost	simple_charts	72
tawk	tawk.to	73
tchgdns	wp-appbox	73
tcoderbd	tcbd_tooltip	73
the-guild	graphql_mesh	74
	graphql_mesh_cli	76
	graphql_mesh_http	77
Theeventscalendar	event_tickets	78
themepoints	super_testimonials	78
Trustwave	modsecurity	79
tusharimran	ablocks	79
ultimatemember	ultimate_member	80
undsgn	uncode	81
unlimited-elements	unlimited_elements_for_elementor	82
vanderwijk	content_blocks	82
vcita	online_payments_-_get_paid_with_paypal\,_square_\&_stripe	83
victorfreitas	wpupper_share_buttons	83
webcodingplace	ultimate_classified_listings	84
webdevocean	3d_photo_gallery	85
	pricing_tables	85

Vendor	Product	Page Number
webdevocean	team_builder	86
webfactoryltd	advanced_google_recaptcha	86
wecantrack	affiliate_links	86
wegia	wegia	87
wow-company	modal_window	94
wpdesk	flexible_wishlist_for_woocommerce	94
wpeverest	everest_forms	95
wpexperts	givewp_square	95
	post_smtp	96
wpindeed	ultimate_learning_pro	96
wpmet	elementskit_elementor_addons	97
wwexgroup	ltl_freight_quotes	97
Xmlsoft	libxml2	98
xootix	login\/signup_popup	98
yawave	yawave	98
yaycommerce	yaysmtp	99
Hardware		
Dlink	dap-1320	100
fiberhome	an5506-01-a	100
	an5506-01a	101
yitechnology	yi_car_dashcam	102
Operating System		
Dlink	dap-1320_firmware	102
fiberhome	an5506-01-a_firmware	103
	an5506-01a_firmware	104
yitechnology	yi_car_dashcam_firmware	104
zephyrproject	zephyr	105

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 1clickmigration					
Product: 1_click_migration					
Affected Version(s): * Up to (including) 2.1					
Exposure of Sensitive Information to an Unauthorized Actor	18-Feb-2025	5.9	The 1 Click WordPress Migration Plugin – 100% FREE for a limited time plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.1 via the class-ocm-backup.php. This makes it possible for unauthenticated attackers to extract sensitive data including usernames and their respective password hashes during a short window of time in which the backup is in process. **CVE ID: CVE-2024-13609**	N/A	A-1CL-1_CL-040325/1
Cross-Site Request Forgery (CSRF)	18-Feb-2025	5.3	The 1 Click WordPress Migration Plugin – 100% FREE for a limited time plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1. This is due to missing or incorrect nonce validation on the cancel_actions() function. This makes it possible for unauthenticated attackers to cancel a triggered backup via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13555**	N/A	A-1CL-1_CL-040325/2
Vendor: adityapatadia					
Product: gumlet_video					

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
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Gumlet Video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gumlet' shortcode in all versions up to, and including, 1.0.3 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-2024-13576**	N/A	A-ADI-GUML-040325/3
Vendor: akashmalik					
Product: scracth_\&_win					
Affected Version(s): * Up to (excluding) 2.9.0					
Missing Authorization	18-Feb-2025	5.3	The Scratch & Win – Giveaways and Contests. Boost subscribers, traffic, repeat visits, referrals, sales and more plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the apmswn_create_discount() function in all versions up to, and including, 2.8.0. This makes it possible for unauthenticated attackers to create coupons. **CVE ID: CVE-2024-13316**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3212730%40scratch-win-giveaways-for-website-facebook&new=3212730%40scratch-win-giveaways-for-website-facebook&sfp_email=&sfph_mail=	A-AKA-SCRA-040325/4
Vendor: amauri					
Product: wpmobile.app					
Affected Version(s): * Up to (excluding) 11.57					
URL Redirection to Untrusted Site ('Open	20-Feb-2025	7.2	The WPMobile.App plugin for WordPress is vulnerable to Open Redirect in all versions up to, and	https://plugins.trac.wordpress.org/changeset/3243366	A-AMA-WPMO-040325/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Redirect')			including, 11.56. This is due to insufficient validation on the redirect URL supplied via the 'redirect' parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action. **CVE ID: CVE-2024-13888**		
Vendor: amothemo					
Product: amo_team_showcase					
Affected Version(s): * Up to (including) 1.1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The AMO Team Showcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's amoteam_skills 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 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-2025-1407**	N/A	A-AMO-AMO_-040325/6
Vendor: backie					
Product: option_editor					
Affected Version(s): * Up to (including) 1.0					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	8.8	The Option Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing nonce validation on the plugin_page() function. This makes it possible for unauthenticated attackers to update arbitrary options	N/A	A-BAC-OPTI-040325/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the WordPress site via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site. **CVE ID: CVE-2024-13852**		
Vendor: bandsintown					
Product: bandsintown					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Bandsintown Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bandsintown_events' shortcode in all versions up to, and including, 1.3.1 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-2024-13802**	N/A	A-BAN-BAND-040325/8
Vendor: benbodhi					
Product: svg_support					
Affected Version(s): * Up to (excluding) 2.5.11					
Improper Neutralization of Input During Web Page	21-Feb-2025	6.4	The SVG Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and	https://plugins.trac.wordpress.org/changeset/3244181/	A-BEN-SVG_-040325/9

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
Generation ('Cross-site Scripting')			including, 2.5.10 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 the SVG file. By default, this can only be exploited by administrators, but the ability to upload SVG files can be extended to authors. **CVE ID: CVE-2024-10222**		
Vendor: better-auth					
Product: better_auth					
Affected Version(s): * Up to (excluding) 1.1.21					
URL Redirection to Untrusted Site ('Open Redirect')	24-Feb-2025	6.1	Better Auth is an authentication and authorization library for TypeScript. Prior to version 1.1.21, the application is vulnerable to an open redirect due to improper validation of the callbackURL parameter in the email verification endpoint and any other endpoint that accepts callback url. While the server blocks fully qualified URLs, it incorrectly allows scheme-less URLs. This results in the browser interpreting the URL as a fully qualified URL, leading to unintended redirection. An attacker can exploit this flaw by crafting a malicious verification link and tricking users into clicking it. Upon successful email verification, the user will be automatically redirected to the attacker's website, which can be used for phishing, malware	https://github.com/better-auth/better-auth/commit/24659aefc35a536b95ea4e5347e52c8803910153, https://github.com/better-auth/better-auth/commit/b381cac7aafd6aa53ef78b6ab771ebfa24643c80	A-BET-BETT-040325/10

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
			distribution, or stealing sensitive authentication tokens. This CVE is a bypass of the fix for GHSA-8jhw-6pjj-8723/CVE-2024-56734. Version 1.1.21 contains an updated patch. **CVE ID: CVE-2025-27143**		
Vendor: bigbuy					
Product: dropshipping_connector_for_woocommerce					
Affected Version(s): * Up to (including) 1.9.19					
Generation of Error Message Containing Sensitive Information	18-Feb-2025	5.3	The BigBuy Dropshipping Connector for WooCommerce plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.9.19. This is due the /vendor/cocur/slugify/bin/generate-default.php file being directly accessible and triggering an error. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website. **CVE ID: CVE-2024-13538**	N/A	A-BIG-DROP-040325/11
Vendor: bishopfox					
Product: sliver					
Affected Version(s): From (including) 1.5.26 Up to (excluding) 1.5.43					
Server-Side Request Forgery (SSRF)	19-Feb-2025	5.3	Sliver is an open source cross-platform adversary emulation/red team framework, it can be used by organizations of all sizes to perform security testing. The reverse port forwarding in sliver	https://github.com/BishopFox/sliver/commit/0f340a25cf3d496ed870dae7da39eab4427bc16f, https://github.com/BishopFox/	A-BIS-SLIV-040325/12

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
			teamserver allows the implant to open a reverse tunnel on the sliver teamserver without verifying if the operator instructed the implant to do so. The only impact that has been shown is the exposure of the server's IP address to a third party. This issue has been addressed in version 1.5.43 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-27090**	sliver/commit/10e245326070c6a5884a02e0790bb7e2baefb3a1, https://github.com/BishopFox/sliver/security/advisories/GHSA-fh4v-v779-4g2w	
Vendor: byconsole					
Product: wooodt_lite					
Affected Version(s): * Up to (including) 2.5.1					
Generation of Error Message Containing Sensitive Information	18-Feb-2025	5.3	The WooODT Lite – Delivery & pickup date time location for WooCommerce plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.5.1. This is due the /inc/bycwooodt_get_all_orders.php file being publicly accessible and generating a publicly visible error message. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website. **CVE ID: CVE-2024-13540**	N/A	A-BYC-WOOO-040325/13
Vendor: carspot_project					
Product: carspot					

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 Version(s): * Up to (excluding) 2.4.4					
Unverified Password Change	18-Feb-2025	9.8	The CarSpot – Dealership Wordpress Classified Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.4.3. This is due to the plugin not properly validating a token prior to updating a user's password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account. **CVE ID: CVE-2024-12860**	N/A	A-CAR-CARS-040325/14
Vendor: catsone					
Product: cats_job_listings					
Affected Version(s): * Up to (including) 2.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The CATS Job Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catsone' shortcode in all versions up to, and including, 2.0.9 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-2024-13577**	N/A	A-CAT-CATS-040325/15
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): * Up to (including) 5.13.0					

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 Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a time-based blind SQL Injection vulnerability in the EditEventTypes functionality. The newCountName parameter is directly concatenated into an SQL query without proper sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion. **CVE ID: CVE-2025-1023**	N/A	A-CHU-CHUR-040325/16
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	8.8	A time-based blind SQL Injection vulnerability exists in the ChurchCRM 5.13.0 and prior EditEventAttendees.php within the EN_tyid parameter. The parameter is directly inserted into an SQL query without proper sanitization, allowing attackers to inject malicious SQL commands. Please note that the vulnerability requires Administrator permissions. This flaw can potentially allow attackers to delay the response, indicating the presence of an SQL injection vulnerability. While it is a time-based blind injection, it can be exploited to gain insights into the underlying database, and with further exploitation, sensitive data could be retrieved.	N/A	A-CHU-CHUR-040325/17

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
			CVE ID: CVE-2025-1132		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.2	A vulnerability exists in ChurchCRM 5.13.0. and prior that allows an attacker to execute arbitrary SQL queries by exploiting a boolean-based and time-based blind SQL Injection vulnerability in the BatchWinnerEntry functionality. The CurrentFundraiser parameter is directly concatenated into an SQL query without sufficient sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion. Please note the vulnerability requires Administrator privileges. **CVE ID: CVE-2025-1135**	N/A	A-CHU-CHUR-040325/18
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.2	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a boolean-based and time-based blind SQL Injection vulnerability in the DonatedItemEditor functionality. The CurrentFundraiser parameter is directly concatenated into an SQL query without sufficient sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion. Please note that this vulnerability requires	N/A	A-CHU-CHUR-040325/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator privileges. **CVE ID: CVE-2025-1134**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.2	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a boolean-based blind SQL Injection vulnerability in the EditEventAttendees functionality. The EID parameter is directly concatenated into an SQL query without proper sanitization, making it susceptible to SQL injection attacks. An attacker can manipulate the query, potentially leading to data exfiltration, modification, or deletion. Please note that this vulnerability requires Administrator privileges. **CVE ID: CVE-2025-1133**	N/A	A-CHU-CHUR-040325/20
Improper Authentication	18-Feb-2025	6.1	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to hijack a user's session by exploiting a Stored Cross Site Scripting (XSS) vulnerability in the Group Editor page. This allows admin users to inject malicious JavaScript in the description field, which captures the session cookie of authenticated users. The cookie can then be sent to an external server, enabling session hijacking. It can also lead to information disclosure, as exposed session cookies can be used to impersonate users and gain unauthorised access to sensitive information.	N/A	A-CHU-CHUR-040325/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-0981		
Improper Authentication	19-Feb-2025	4.8	A vulnerability exists in ChurchCRM 5.13.0 that allows an attacker to execute arbitrary JavaScript in a victim's browser via Reflected Cross-Site Scripting (XSS) in the EditEventAttendees.php page. This requires Administration privileges and affects the EID parameter. The flaw allows an attacker to steal session cookies, perform actions on behalf of an authenticated user, and gain unauthorized access to the application. **CVE ID: CVE-2025-1024**	N/A	A-CHU-CHUR-040325/22
Vendor: Cisco					
Product: openh264					
Affected Version(s): * Up to (excluding) 2.6.0					
Heap-based Buffer Overflow	20-Feb-2025	7.5	OpenH264 is a free license codec library which supports H.264 encoding and decoding. A vulnerability in the decoding functions of OpenH264 codec library could allow a remote, unauthenticated attacker to trigger a heap overflow. This vulnerability is due to a race condition between a Sequence Parameter Set (SPS) memory allocation and a subsequent non Instantaneous Decoder Refresh (non-IDR) Network Abstraction Layer (NAL) unit memory usage. An attacker could exploit this vulnerability by crafting a malicious bitstream and tricking a victim user into processing an arbitrary video containing the malicious bistream. An	https://github.com/cisco/openh264/security/advisories/GHSA-m99q-5j7x-7m9x	A-CIS-OPEN-040325/23

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
			exploit could allow the attacker to cause an unexpected crash in the victim's user decoding client and, possibly, perform arbitrary commands on the victim's host by abusing the heap overflow. This vulnerability affects OpenH264 2.5.0 and earlier releases. Both Scalable Video Coding (SVC) mode and Advanced Video Coding (AVC) mode are affected by this vulnerability. OpenH264 software releases 2.6.0 and later contained the fix for this vulnerability. Users are advised to upgrade. There are no known workarounds for this vulnerability. ### For more information If you have any questions or comments about this advisory: * [Open an issue in cisco/openh264](https://github.com/cisco/openh264/issues) * Email Cisco Open Source Security (oss-security@cisco.com) and Cisco PSIRT (psirt@cisco.com) ### Credits: * **Research:** Octavian Guzu and Andrew Calvano of Meta * **Fix ideation:** Philipp Hancke and Shyam Sadhwani of Meta * **Fix implementation:** Benzheng Zhang (@BenzhengZhang) * **Release engineering:**		

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
			Benzheng Zhang (@BenzhengZhang) **CVE ID: CVE-2025-27091**		
Vendor: clavaque					
Product: s2member					
Affected Version(s): * Up to (excluding) 250214					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.1	The s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 241114. 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-2024-11376**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3240794%40s2member&new=3240794%40s2member&sfp_email=&sfph_mail=#file1	A-CLA-S2ME-040325/24
Vendor: cmseasy					
Product: cmseasy					
Affected Version(s): 7.7.7.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2025	4.3	A vulnerability has been found in CmsEasy 7.7.7.9 and classified as problematic. Affected by this vulnerability is the function deleteimg_action in the library lib/admin/image_admin.php. The manipulation of the argument imgname leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor	N/A	A-CMS-CMSE-040325/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1336**		
Vendor: CMU					
Product: ghosts					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.2.7.90					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Feb-2025	7.5	GHOSTS is an open source user simulation framework for cyber experimentation, simulation, training, and exercise. A path traversal vulnerability was discovered in GHOSTS version 8.0.0.0 that allows an attacker to access files outside of the intended directory through the photo retrieval endpoint. The vulnerability exists in the /api/npcs/{id}/photo endpoint, which is designed to serve profile photos for NPCs (Non-Player Characters) but fails to properly validate and sanitize file paths. When an NPC is created with a specially crafted photoLink value containing path traversal sequences (../, ..\, etc.), the application processes these sequences without proper sanitization. This allows an attacker to traverse directory structures and access files outside of the intended photo directory, potentially exposing sensitive system files. The vulnerability is particularly severe because it allows reading arbitrary files from the server's filesystem with the permissions of the web application process, which could include configuration files, credentials, or other	https://github.com/cmu-sei/GHOSTS/commit/e69827556a52ff813de00e1017c4b62598d2c887, https://github.com/cmu-sei/GHOSTS/security/advisories/GHSA-qr67-m6w9-wj3j	A-CMU-GHOS-040325/26

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
			sensitive data. This issue has been addressed in version 8.2.7.90 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-27092**		
Vendor: code-projects					
Product: blood_bank_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2025	3.5	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /Blood/A-.php. The manipulation of the argument Bloodname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1586**	N/A	A-COD-BLOO-040325/27
Vendor: codemenschen					
Product: gift_vouchers					
Affected Version(s): * Up to (including) 4.4.6					
Missing Authorization	20-Feb-2025	5.3	The Gift Cards (Gift Vouchers and Packages) (WooCommerce Supported) plugin for WordPress is vulnerable to unauthorized modification of data|loss of data due to a missing capability check on the 'update_voucher_price', 'update_voucher_date', 'update_voucher_note' functions in all versions up to, and including, 4.4.6. This makes it possible for unauthenticated attackers to update the value, expiration date, and user	N/A	A-COD-GIFT-040325/28

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
			note for any gift voucher. **CVE ID: CVE-2024-13520**		
Vendor: Combodo					
Product: itop					
Affected Version(s): * Up to (excluding) 2.7.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2025	6.8	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.12, 3.1.2, and 3.2.0 are vulnerable to cross-site scripting when the preferences page is opened. Versions 2.7.12, 3.1.2, and 3.2.0 fix the issue. **CVE ID: CVE-2025-27139**	https://github.com/Combodo/iTop/security/advisories/GHSA-c6mg-9537-c8cf	A-COM-ITOP-040325/29
Affected Version(s): 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2025	6.8	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.12, 3.1.2, and 3.2.0 are vulnerable to cross-site scripting when the preferences page is opened. Versions 2.7.12, 3.1.2, and 3.2.0 fix the issue. **CVE ID: CVE-2025-27139**	https://github.com/Combodo/iTop/security/advisories/GHSA-c6mg-9537-c8cf	A-COM-ITOP-040325/30
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2025	6.8	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.12, 3.1.2, and 3.2.0 are vulnerable to cross-site scripting when the preferences page is opened. Versions 2.7.12, 3.1.2, and 3.2.0 fix the issue. **CVE ID: CVE-2025-27139**	https://github.com/Combodo/iTop/security/advisories/GHSA-c6mg-9537-c8cf	A-COM-ITOP-040325/31
Vendor: covertnine					
Product: c9_admin_dashboard					
Affected Version(s): * Up to (including) 1.3.5					
Improper Neutralizati	21-Feb-2025	6.4	The C9 Admin Dashboard plugin for WordPress is	N/A	A-COV-C9_A-040325/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.3.5 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 the SVG file. **CVE ID: CVE-2024-13379**		
Product: c9_blocks					
Affected Version(s): * Up to (including) 1.7.7					
Generation of Error Message Containing Sensitive Information	21-Feb-2025	5.3	The C9 Blocks plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.7.7. This is due the plugin containing a publicly accessible composer-setup.php file with error display enabled. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website. **CVE ID: CVE-2024-13537**	N/A	A-COV-C9_B-040325/33
Vendor: cyberchimps					
Product: responsive_addons_for_elementor					
Affected Version(s): * Up to (excluding) 1.6.5					
Improper Control of Filename for Include/Require	21-Feb-2025	8.8	The Responsive Addons for Elementor – Free Elementor Addons Plugin and Elementor Templates plugin for WordPress is	https://plugins.trac.wordpress.org/changeset/3226779/responsive-addons-for-	A-CYB-RESP-040325/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Statement in PHP Program ('PHP Remote File Inclusion')			vulnerable to Local File Inclusion in all versions up to, and including, 1.6.4 via several widgets. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. **CVE ID: CVE-2024-13353**	elementor/tags/1.6.5/includes/widgets-manager/widgets/woocommerce/class-responsive-addons-for-elementor-product-carousel.php	
Vendor: dcurasi					
Product: cookie_notice_bar					
Affected Version(s): * Up to (including) 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	5.5	The Cookie Notice Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID: CVE-2024-13849**	N/A	A-DCU-COOK-040325/35
Vendor: debounce					
Product: email_validator					
Affected Version(s): * Up to (including) 5.6.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	19-Feb-2025	6.1	The DeBounce Email Validator plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.6.6. This is due to missing or incorrect nonce validation on the 'debounce_email_validator' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13339**	N/A	A-DEB-EMAI-040325/36
Vendor: elementor					
Product: website_builder					
Affected Version(s): * Up to (excluding) 3.27.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the border, margin and gap parameters in all versions up to, and including, 3.27.4 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-2024-13445**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3241278%40elementor%2Ftrunk&old=3239949%40elementor%2Ftrunk&sfp_email=&sfph_mail=	A-ELE-WEBS-040325/37
Vendor: eniture					
Product: ltl_freight_quotes					
Affected Version(s): * Up to (excluding) 2.2.11					
Improper	19-Feb-2025	7.5	The LTL Freight Quotes –	https://plugins.t	A-ENI-LTL_-

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
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			SAIA Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 2.2.10 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-2024-13483**	rac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3242171%40ltl-freight-quotes-saia-edition&new=3242171%40ltl-freight-quotes-saia-edition&sfp_email=&sfph_mail=	040325/38
Affected Version(s): * Up to (excluding) 2.3.12					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Feb-2025	7.5	The LTL Freight Quotes – GlobalTranz Edition plugin for WordPress is vulnerable to SQL Injection via the 'engtz_wd_save_dropship' AJAX endpoint in all versions up to, and including, 2.3.11 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-2024-13476**	https://plugins.trac.wordpress.org/changeset/3242457/	A-ENI-LTL_-040325/39
Affected Version(s): * Up to (excluding) 3.2.5					
Improper Neutralization of Special	19-Feb-2025	7.5	The LTL Freight Quotes – SEFL Edition plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset?sf	A-ENI-LTL_-040325/40

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
Elements used in an SQL Command ('SQL Injection')			SQL Injection via the 'dropship_edit_id' and 'edit_id' parameters in all versions up to, and including, 3.2.4 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-2024-13479**	p_email=&sfph_mail=&reponame=&old=3242634%40ltl-freight-quotes-sefl-edition&new=3242634%40ltl-freight-quotes-sefl-edition&sfp_email=&sfph_mail=	
Affected Version(s): * Up to (excluding) 3.3.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.5	The LTL Freight Quotes – ABF Freight Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 3.3.7 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-2024-13485**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3242640%40ltl-freight-quotes-abf-freight-edition&new=3242640%40ltl-freight-quotes-abf-freight-edition&sfp_email=&sfph_mail=	A-ENI-LTL_-040325/41
Affected Version(s): * Up to (excluding) 3.6.5					
Improper Neutralization of Special Elements used in an	19-Feb-2025	7.5	The LTL Freight Quotes – TForce Edition plugin for WordPress is vulnerable to SQL Injection via the 'dropship_edit_id' and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponam	A-ENI-LTL_-040325/42

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
SQL Command ('SQL Injection')			'edit_id' parameters in all versions up to, and including, 3.6.4 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-2024-13478**	e=&old=3242156%40ltl-freight-quotes-ups-edition&new=3242156%40ltl-freight-quotes-ups-edition&sfp_email=&sfph_mail=	
Affected Version(s): * Up to (excluding) 4.2.11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.5	The LTL Freight Quotes – Old Dominion Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 4.2.10 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-2024-13489**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3242160%40ltl-freight-quotes-odfl-edition&new=3242160%40ltl-freight-quotes-odfl-edition&sfp_email=&sfph_mail=	A-ENI-LTL_-040325/43
Product: small_package_quotes					
Affected Version(s): * Up to (excluding) 1.3.6					
Improper Neutralization of Special Elements used in an SQL	19-Feb-2025	7.5	The Small Package Quotes – USPS Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' parameter in all versions up to, and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=324206	A-ENI-SMAL-040325/44

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
Command ('SQL Injection')			including, 1.3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-13533**	0%40small-package-quotes-usps-edition&new=3242060%40small-package-quotes-usps-edition&sfp_email=&sfph_mail=	
Affected Version(s): * Up to (excluding) 4.3.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.5	The Small Package Quotes – For Customers of FedEx plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 4.3.1 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-2024-13491**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3242108%40small-package-quotes-fedex-edition&new=3242108%40small-package-quotes-fedex-edition&sfp_email=&sfph_mail=	A-ENI-SMAL-040325/45
Affected Version(s): * Up to (excluding) 5.2.19					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2025	7.5	The Small Package Quotes – Worldwide Express Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 5.2.18 due to insufficient escaping	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3241919%40small-package-quotes-wwe-	A-ENI-SMAL-040325/46

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
			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-2024-13534**	edition&new=3241919%40small-package-quotes-wwe-edition&sfp_email=&sfph_mail=	
Vendor: ex-themes					
Product: woocommerce_food					
Affected Version(s): * Up to (excluding) 3.3.3					
Improper Control of Generation of Code ('Code Injection')	20-Feb-2025	7.3	The WooCommerce Food - Restaurant Menu & Food ordering plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.3.2. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes. **CVE ID: CVE-2024-13792**	N/A	A-EX--WOOC-040325/47
Vendor: fabianros					
Product: real_estate_property_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Feb-2025	6.3	A vulnerability classified as critical has been found in code-projects Real Estate Property Management System 1.0. This affects an unknown part of the file /search.php. The manipulation of the argument	N/A	A-FAB-REAL-040325/48

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
			StateName/CityName/Area Name/CatId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1374**		
Vendor: formassembly					
Product: wp-formassembly					
Affected Version(s): * Up to (including) 2.0.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The WP-FormAssembly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'formassembly' shortcode in all versions up to, and including, 2.0.11 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-2024-13501**	N/A	A-FOR-WP-F-040325/49
Vendor: Genetechsolutions					
Product: pie_register					
Affected Version(s): * Up to (including) 3.8.3.9					
Insertion of Sensitive Information into Log File	21-Feb-2025	5.3	The Registration Forms – User Registration Forms, Invitation-Based Registrations, Front-end User Profile, Login Form & Content Restriction plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.8.3.9 through publicly exposed log files. This makes it possible for	N/A	A-GEN-PIE_-040325/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to view potentially sensitive information about users contained in the exposed log files. **CVE ID: CVE-2024-13818**		
Vendor: Glpi-project					
Product: glpi					
Affected Version(s): * Up to (excluding) 10.0.18					
Exposure of Sensitive Information to an Unauthorized Actor	25-Feb-2025	6.5	GLPI is a free asset and IT management software package. Prior to version 10.0.18, a low privileged user can enable debug mode and access sensitive information. Version 10.0.18 contains a patch. As a workaround, one may delete the `install/update.php` file. **CVE ID: CVE-2025-25192**	N/A	A-GLP-GLPI-040325/51
Affected Version(s): From (including) 9.5.0 Up to (excluding) 10.0.18					
Incorrect Implementation of Authentication Algorithm	25-Feb-2025	7.5	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.18, if a "Mail servers" authentication provider is configured to use an Oauth connection provided by the OauthIMAP plugin, anyone can connect to GLPI using a user name on which an Oauth authorization has already been established. Version 10.0.18 contains a patch. As a workaround, one may disable any "Mail servers" authentication provider configured to use an Oauth connection provided by the OauthIMAP plugin. **CVE ID: CVE-2025-23046**	N/A	A-GLP-GLPI-040325/52
Vendor: goodlayers					

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
Product: tour_master					
Affected Version(s): * Up to (excluding) 5.3.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	6.5	The Tour Master - Tour Booking, Travel, Hotel plugin for WordPress is vulnerable to time-based SQL Injection via the 'review_id' parameter in all versions up to, and including, 5.3.6 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 Subscriber-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-2024-13369**	N/A	A-GOO-TOUR-040325/53
Vendor: haozhexie					
Product: wp-bibtex					
Affected Version(s): * Up to (including) 3.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The WP-BibTeX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'WpBibTeX' shortcode in all versions up to, and including, 3.0.1 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-2024-13578**	N/A	A-HAO-WP-B-040325/54

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
Vendor: homeasap					
Product: easy_mls_listings_import					
Affected Version(s): * Up to (excluding) 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Easy MLS Listings Import plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'homeasap-featured-listings' shortcode in all versions up to, and including, 2.0.1 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-2024-12525**	N/A	A-HOM-EASY-040325/55
Vendor: icopydoc					
Product: maps_for_wp					
Affected Version(s): * Up to (excluding) 1.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The Maps for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'MapOnePoint' shortcode in all versions up to, and including, 1.2.4 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-2024-13648**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3226414%40maps-for-wp&new=3226414%40maps-for-wp&sfp_email=&sfph_mail=	A-ICO-MAPS-040325/56

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
Vendor: igumbi					
Product: igumbi					
Affected Version(s): * Up to (excluding) 1.41					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The igumbi Online Booking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'igumbi_calendar' shortcode in all versions up to, and including, 1.40 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-2024-13455**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3243431%40igumbi-online-booking&new=3243431%40igumbi-online-booking&sfp_email=&sfph_mail=	A-IGU-IGUM-040325/57
Vendor: imaginate-solutions					
Product: file_uploads_addon_for_woocommerce					
Affected Version(s): * Up to (including) 1.7.1					
Exposure of Sensitive Information to an Unauthorized Actor	18-Feb-2025	7.5	The File Uploads Addon for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.7.1 via the 'uploads' directory. This makes it possible for unauthenticated attackers to extract sensitive data stored insecurely in the /wp-content/uploads directory which can contain file attachments uploaded by customers. **CVE ID: CVE-2024-13622**	N/A	A-IMA-FILE-040325/58
Vendor: imamura					
Product: newpost_catch					
Affected Version(s): * Up to (including) 1.3.19					

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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The Newpost Catch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's npc shortcode in all versions up to, and including, 1.3.19 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-2025-1406**	N/A	A-IMA-NEWP-040325/59
Vendor: iptanus					
Product: wordpress_file_upload					
Affected Version(s): * Up to (excluding) 4.25.3					
Cross-Site Request Forgery (CSRF)	25-Feb-2025	4.3	The WordPress File Upload plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.25.2. This is due to missing or incorrect nonce validation on the 'wfu_file_details' function. This makes it possible for unauthenticated attackers to modify user data details associated with uploaded files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13494**	https://plugins.trac.wordpress.org/changeset/3241028/wp-file-upload	A-IPT-WORD-040325/60
Vendor: istmoplugins					
Product: get_bookings_wp					
Affected Version(s): * Up to (including) 1.1.27					
Missing Authorizatio	18-Feb-2025	8.8	The GetBookingsWP – Appointments Booking	N/A	A-IST-GET_-040325/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n			Calendar Plugin For WordPress plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.1.27. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for authenticated attackers, with subscriber-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account. **CVE ID: CVE-2024-13677**		
Vendor: jakob42					
Product: reaction_buttons					
Affected Version(s): * Up to (including) 2.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	5.5	The Reaction Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID: CVE-2024-13848**	N/A	A-JAK-REAC-040325/62

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
Vendor: janobe					
Product: e-learning_system					
Affected Version(s): 1.0					
Improper Access Control	23-Feb-2025	4.7	A vulnerability was found in SourceCodester E-Learning System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/modules/lesson/index.php of the component List of Lessons Page. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. **CVE ID: CVE-2025-1590**	N/A	A-JAN-E-LE-040325/63
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2025	4.3	A vulnerability was found in SourceCodester E-Learning System 1.0 and classified as problematic. This issue affects some unknown processing of the file /register.php of the component User Registration Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. **CVE ID: CVE-2025-1589**	N/A	A-JAN-E-LE-040325/64
Vendor: jonathanjernigan					
Product: pie_calendar					
Affected Version(s): * Up to (excluding) 1.2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The Events Calendar Made Simple – Pie Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's piecal shortcode in all versions up to, and including, 1.2.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/3243992/	A-JON-PIE_-040325/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2025-1410**		
Vendor: keap					
Product: keap_official_opt_in_forms					
Affected Version(s): * Up to (including) 2.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Feb-2025	9.8	The Keap Official Opt-in Forms plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.0.1 via the service parameter. This makes it possible for unauthenticated attackers to include PHP files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where PHP files can be uploaded and included. If register_argc_argv is enabled on the server and pearcmd.php is installed, this issue might lead to Remote Code Execution. **CVE ID: CVE-2024-13725**	https://plugins.trac.wordpress.org/browser/infusionsoft-official-opt-in-forms/trunk/infusionsoft.php#L2540	A-KEA-KEAP-040325/66
Vendor: kerryoco					
Product: threepress					
Affected Version(s): * Up to (excluding) 1.7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Threepress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'threepress' shortcode in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output	N/A	A-KER-THRE-040325/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-13395**		
Vendor: kevinbrent					
Product: wprequal					
Affected Version(s): * Up to (including) 8.2.10					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	4.3	The Mortgage Lead Capture System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 8.2.10. This is due to missing or incorrect nonce validation on the 'wprequal_reset_defaults' action. This makes it possible for unauthenticated attackers to reset the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2025-0796**	N/A	A-KEV-WPRE-040325/68
Vendor: Kriesi					
Product: enfold					
Affected Version(s): * Up to (excluding) 7.0					
Improper Access Control	25-Feb-2025	5.3	The Enfold theme for WordPress is vulnerable to unauthorized access of data due to a missing capability check in avia-export-class.php in all versions up to, and including, 6.0.9. This makes it possible for unauthenticated attackers to export all avia settings which may included	N/A	A-KRI-ENFO-040325/69

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
			sensitive information such as the Mailchimp API Key, reCAPTCHA Secret Key, or Envato private token if they are set. **CVE ID: CVE-2024-13693**		
Affected Version(s): * Up to (excluding) 7.0.0					
Server-Side Request Forgery (SSRF)	25-Feb-2025	6.4	The Enfold theme for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.0.9 via the 'attachment_id' parameter. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. **CVE ID: CVE-2024-13695**	N/A	A-KRI-ENFO-040325/70
Vendor: legoeso					
Product: pdf_manager					
Affected Version(s): * Up to (including) 1.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Feb-2025	6.5	The Legoeso PDF Manager plugin for WordPress is vulnerable to time-based SQL Injection via the ‘checkedVals’ parameter in all versions up to, and including, 1.2.2 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 Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from	N/A	A-LEG-PDF_-040325/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the database. **CVE ID: CVE-2025-0866**		
Vendor: lightspeedhq					
Product: ecwid_ecommerce_shopping_cart					
Affected Version(s): * Up to (excluding) 6.12.28					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	4.3	The Ecwid by Lightspeed Ecommerce Shopping Cart plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.12.27. This is due to missing or incorrect nonce validation on the ecwid_deactivate_feedback() function. This makes it possible for unauthenticated attackers to send deactivation messages on behalf of a site owner via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13795**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3241777%40ecwid-shopping-cart&new=3241777%40ecwid-shopping-cart&sfp_email=&sfph_mail=	A-LIG-ECWI-040325/72
Vendor: lmxcms					
Product: lmxcms					
Affected Version(s): 1.41					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Feb-2025	4.1	A vulnerability, which was classified as problematic, was found in lmxcms 1.41. Affected is an unknown function of the file db.inc.php of the component Maintenance. The manipulation leads to code injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early	N/A	A-LMX-LMXC-040325/73

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
			about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1465**		
Vendor: localsend					
Product: localsend					
Affected Version(s): * Up to (excluding) 1.17.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Feb-2025	8.8	LocalSend is a free, open-source app that allows users to securely share files and messages with nearby devices over their local network without needing an internet connection. Prior to version 1.17.0, due to the missing sanitization of the path in the `POST /api/localsend/v2/prepare-upload` and the `POST /api/localsend/v2/upload` endpoint, a malicious file transfer request can write files to the arbitrary location on the system, resulting in the remote command execution. A malicious file transfer request sent by nearby devices can write files into an arbitrary directory. This usually allows command execution via the startup folder on Windows or Bash-related files on Linux. If the user enables the `Quick Save` feature, it will silently write files without explicit user interaction. Version 1.17.0 fixes this issue. **CVE ID: CVE-2025-27142**	https://github.com/localsend/localsend/commit/e8635204ec782ded45bc7d698deb60f3c4105687, https://github.com/localsend/localsend/security/advisories/GHSA-f7jp-p6j4-3522	A-LOC-LOCA-040325/74
Vendor: magayo					
Product: magayo_lottery_results					
Affected Version(s): * Up to (including) 2.0.12					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	6.1	The magayo Lottery Results plugin for WordPress is vulnerable to Cross-Site Request Forgery in all	N/A	A-MAG-MAGA-040325/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 2.0.12. This is due to missing or incorrect nonce validation on the 'magayo-lottery-results' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13522**		
Vendor: magazine3					
Product: web_stories_enhancer					
Affected Version(s): * Up to (excluding) 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Web Stories Enhancer – Level Up Your Web Stories plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'web_stories_enhancer' shortcode in all versions up to, and including, 1.3 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-2024-13575**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3238312%40web-stories-enhancer&new=3238312%40web-stories-enhancer&sfp_email=&sfph_mail=	A-MAG-WEB_-040325/76
Vendor: marcoingraiti					
Product: actionwear_products_sync					
Affected Version(s): * Up to (excluding) 2.3.3					
Generation of Error Message Containing	18-Feb-2025	5.3	The Actionwear products sync plugin for WordPress is vulnerable to Full Path Disclosure in all versions up	N/A	A-MAR-ACTI-040325/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			to, and including, 2.3.0. This is due the composer-setup.php file being publicly accessible with 'display_errors' set to true. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website. **CVE ID: CVE-2024-13535**		
Vendor: matiskiba					
Product: ravpage					
Affected Version(s): * Up to (including) 2.31					
Deserialization of Untrusted Data	20-Feb-2025	9.8	The ravpage plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.31 via deserialization of untrusted input from the 'paramsv2' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. **CVE ID: CVE-2024-13789**	N/A	A-MAT-RAVP-040325/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: mayurik					
Product: best_church_management_software					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Feb-2025	7.3	A vulnerability was found in SourceCodester Best Church Management Software 1.0 and classified as critical. This issue affects some unknown processing of the file /fpassword.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1596**	N/A	A-MAY-BEST-040325/79
Improper Access Control	24-Feb-2025	6.3	A vulnerability was found in SourceCodester Best Church Management Software 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/app/asset_crud.php. The manipulation of the argument photo1 leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1598**	N/A	A-MAY-BEST-040325/80
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2025	3.5	A vulnerability was found in SourceCodester Best Church Management Software 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/redirect.php. The manipulation of the	N/A	A-MAY-BEST-040325/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument a leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1597**		
Product: best_employee_management_system					
Affected Version(s): 1.0					
Improper Access Control	23-Feb-2025	4.7	A vulnerability classified as critical has been found in SourceCodester Best Employee Management System 1.0. This affects an unknown part of the file /_hr_soft/assets/uploadImage/Profile/ of the component Profile Picture Handler. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. **CVE ID: CVE-2025-1593**	N/A	A-MAY-BEST-040325/82
Exposure of Sensitive Information to an Unauthorized Actor	24-Feb-2025	4.3	A vulnerability classified as problematic was found in SourceCodester Best Employee Management System 1.0. This vulnerability affects unknown code of the file /admin/backup/backups.php. The manipulation leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1606**	N/A	A-MAY-BEST-040325/83
Improper Neutralization of Input	23-Feb-2025	2.4	A vulnerability was found in SourceCodester Best Employee Management	N/A	A-MAY-BEST-040325/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/Operations/Role.php of the component Add Role Page. The manipulation of the argument assign_name/description leads to cross site scripting. The attack may be launched remotely. **CVE ID: CVE-2025-1592**		
Vendor: megaoptim					
Product: rapid_cache					
Affected Version(s): * Up to (including) 1.2.3					
Use of Cache Containing Sensitive Information	18-Feb-2025	7.2	The Rapid Cache plugin for WordPress is vulnerable to Cache Poisoning in all versions up to, and including, 1.2.3. This is due to plugin storing HTTP headers in the cached data. This makes it possible for unauthenticated attackers to poison the cache with custom HTTP headers that may be unsanitized which can lead to Cross-Site Scripting. **CVE ID: CVE-2024-12314**	N/A	A-MEG-RAPI-040325/85
Vendor: metabase					
Product: metabase					
Affected Version(s): From (including) 1.47.0 Up to (excluding) 1.50.36					
Incorrect Permission Assignment for Critical Resource	24-Feb-2025	6.5	Metabase Enterprise Edition is the enterprise version of Metabase business intelligence and data analytics software. Starting in version 1.47.0 and prior to versions 1.50.36, 1.51.14, 1.52.11, and 1.53.2 of Metabase Enterprise Edition, users	https://github.com/metabase/metabase/security/advisories/GHSA-6cc4-h534-xh5p	A-MET-META-040325/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with impersonation permissions may be able to see results of cached questions, even if their permissions don’t allow them to see the data. If some user runs a question which gets cached, and then an impersonated user runs that question, then the impersonated user sees the same results as the previous user. These cached results may include data the impersonated user should not have access to. This vulnerability only impacts the Enterprise Edition of Metabase and not the Open Source Edition. Versions 1.53.2, 1.52.11, 1.51.14, and 1.50.36 contains a patch. Versions on the 1.49.X, 1.48.X, and 1.47.X branches are vulnerable but do not have a patch available, so users should upgrade to a major version with an available fix. Disabling question caching is a workaround for this issue. **CVE ID: CVE-2025-27141**		
Affected Version(s): From (including) 1.51.0 Up to (excluding) 1.51.14					
Incorrect Permission Assignment for Critical Resource	24-Feb-2025	6.5	Metabase Enterprise Edition is the enterprise version of Metabase business intelligence and data analytics software. Starting in version 1.47.0 and prior to versions 1.50.36, 1.51.14, 1.52.11, and 1.53.2 of Metabase Enterprise Edition, users with impersonation permissions may be able to see results of cached questions, even if their permissions don’t allow them to see the data. If some user runs a question	https://github.com/metabase/metabase/security/advisories/GHSA-6cc4-h534-xh5p	A-MET-META-040325/87

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
			which gets cached, and then an impersonated user runs that question, then the impersonated user sees the same results as the previous user. These cached results may include data the impersonated user should not have access to. This vulnerability only impacts the Enterprise Edition of Metabase and not the Open Source Edition. Versions 1.53.2, 1.52.11, 1.51.14, and 1.50.36 contains a patch. Versions on the 1.49.X, 1.48.X, and 1.47.X branches are vulnerable but do not have a patch available, so users should upgrade to a major version with an available fix. Disabling question caching is a workaround for this issue. **CVE ID: CVE-2025-27141**		
Affected Version(s): From (including) 1.52.0 Up to (excluding) 1.52.11					
Incorrect Permission Assignment for Critical Resource	24-Feb-2025	6.5	Metabase Enterprise Edition is the enterprise version of Metabase business intelligence and data analytics software. Starting in version 1.47.0 and prior to versions 1.50.36, 1.51.14, 1.52.11, and 1.53.2 of Metabase Enterprise Edition, users with impersonation permissions may be able to see results of cached questions, even if their permissions don't allow them to see the data. If some user runs a question which gets cached, and then an impersonated user runs that question, then the impersonated user sees the same results as the previous user. These cached results may include data the	https://github.com/metabase/metabase/security/advisories/GHSA-6cc4-h534-xh5p	A-MET-META-040325/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impersonated user should not have access to. This vulnerability only impacts the Enterprise Edition of Metabase and not the Open Source Edition. Versions 1.53.2, 1.52.11, 1.51.14, and 1.50.36 contains a patch. Versions on the 1.49.X, 1.48.X, and 1.47.X branches are vulnerable but do not have a patch available, so users should upgrade to a major version with an available fix. Disabling question caching is a workaround for this issue. **CVE ID: CVE-2025-27141**		
Affected Version(s): From (including) 1.53.0 Up to (excluding) 1.53.2					
Incorrect Permission Assignment for Critical Resource	24-Feb-2025	6.5	Metabase Enterprise Edition is the enterprise version of Metabase business intelligence and data analytics software. Starting in version 1.47.0 and prior to versions 1.50.36, 1.51.14, 1.52.11, and 1.53.2 of Metabase Enterprise Edition, users with impersonation permissions may be able to see results of cached questions, even if their permissions don't allow them to see the data. If some user runs a question which gets cached, and then an impersonated user runs that question, then the impersonated user sees the same results as the previous user. These cached results may include data the impersonated user should not have access to. This vulnerability only impacts the Enterprise Edition of Metabase and not the Open Source Edition. Versions 1.53.2, 1.52.11, 1.51.14, and	https://github.com/metabase/metabase/security/advisories/GHSA-6cc4-h534-xh5p	A-MET-META-040325/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.50.36 contains a patch. Versions on the 1.49.X, 1.48.X, and 1.47.X branches are vulnerable but do not have a patch available, so users should upgrade to a major version with an available fix. Disabling question caching is a workaround for this issue. **CVE ID: CVE-2025-27141**		
Vendor: metagauss					
Product: profilegrid					
Affected Version(s): * Up to (excluding) 5.9.4.3					
Server-Side Request Forgery (SSRF)	18-Feb-2025	5.4	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Limited Server-Side Request Forgery in all versions up to, and including, 5.9.4.2 via the pm_upload_image function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to download and view images, as well as validating if a non-image file exists, both on local or remote hosts. **CVE ID: CVE-2024-13741**	N/A	A-MET-PROF-040325/90
Authorization Bypass Through User-Controlled Key	18-Feb-2025	4.3	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.9.4.2 via the pm_messenger_show_messages function due to missing validation on a user controlled key. This makes	N/A	A-MET-PROF-040325/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it possible for authenticated attackers, with Subscriber-level access and above, to read private conversations of other users. **CVE ID: CVE-2024-13740**		
Vendor: Microsoft					
Product: power_pages					
Affected Version(s): -					
Improper Access Control	19-Feb-2025	8.2	An improper access control vulnerability in Power Pages allows an unauthorized attacker to elevate privileges over a network potentially bypassing the user registration control. This vulnerability has already been mitigated in the service and all affected customers have been notified. This update addressed the registration control bypass. Affected customers have been given instructions on reviewing their sites for potential exploitation and clean up methods. If you've not been notified this vulnerability does not affect you. **CVE ID: CVE-2025-24989**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24989	A-MIC-POWE-040325/92
Vendor: minicoursegenerator					
Product: mini_course_generator					
Affected Version(s): * Up to (excluding) 1.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The Mini Course Generator | Embed mini-courses and interactive content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mcg' shortcode in all versions up to, and including, 1.0.5 due to insufficient input sanitization and output	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3243023%40mini-course-generator&new=3243023%40mini-course-	A-MIN-MINI-040325/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-13672**	generator&sfp_email=&sfph_mail=	
Vendor: mlcalc					
Product: mortgage_loan_calculator					
Affected Version(s): * Up to (including) 1.5.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Mortgage Calculator / Loan Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mlcalc' shortcode in all versions up to, and including, 1.5.20 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-2025-0805**	N/A	A-MLC-MORT-040325/94
Vendor: modalsurvey					
Product: simple_signup_form					
Affected Version(s): * Up to (including) 1.6.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	6.5	The Simple Signup Form plugin for WordPress is vulnerable to SQL Injection via the 'id' attribute of the 'ssf' shortcode in all versions up to, and including, 1.6.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing	N/A	A-MOD-SIMP-040325/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-13595**		
Vendor: modernasistemas					
Product: modernanet					
Affected Version(s): * Up to (excluding) 1.1.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-Feb-2025	7.3	A vulnerability was found in Benner ModernaNet up to 1.1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /Home/JS_CarregaCombo?formName=DADOS_PESSOAIS_PLANO&additionalCondition=&insideParameters=&elementToReturn=DADOS_PESSOAIS_PLANO&ordenarPelaDescricao=true&direcaoOrdenacao=asc&_=1739290047295. The manipulation leads to sql injection. The attack may be launched remotely. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component. **CVE ID: CVE-2025-1640**	N/A	A-MOD-MODE-040325/96
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-Feb-2025	7.3	A vulnerability was found in Benner ModernaNet up to 1.1.0. It has been classified as critical. This affects an unknown part of the file /AGE0000700/GetHorariosDoDia?idespec=0&idproced=1103&data=2025-02-25+19%3A25&agserv=0&convenio=1&localatend=1&idplano=5&pesfis=01&idpro	N/A	A-MOD-MODE-040325/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fissional=0&target=.horarios--dia--d0&_=1739371223797. The manipulation leads to sql injection. It is possible to initiate the attack remotely. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component. **CVE ID: CVE-2025-1641**		
Cross-Site Request Forgery (CSRF)	25-Feb-2025	4.3	A vulnerability was found in Benner ModernaNet up to 1.1.0. It has been rated as problematic. This issue affects some unknown processing of the file /DadosPessoais/SG_AlterarSenha. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component. **CVE ID: CVE-2025-1643**	N/A	A-MOD-MODE-040325/98
Improper Control of Resource Identifiers ('Resource Injection')	25-Feb-2025	4.3	A vulnerability was found in Benner ModernaNet up to 1.1.0. It has been declared as critical. This vulnerability affects unknown code of the file /AGE0000700/GetImageMedico?fooId=1. The manipulation of the argument fooId leads to improper control of resource identifiers. The attack can be initiated remotely. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component. **CVE ID: CVE-2025-1642**	N/A	A-MOD-MODE-040325/99

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
Affected Version(s): * Up to (excluding) 1.2.1					
Cross-Site Request Forgery (CSRF)	25-Feb-2025	4.3	A vulnerability classified as problematic has been found in Benner ModernaNet up to 1.2.0. Affected is an unknown function of the file /DadosPessoais/SG_Gravar. The manipulation of the argument idItAg leads to cross-site request forgery. It is possible to launch the attack remotely. Upgrading to version 1.2.1 is able to address this issue. It is recommended to upgrade the affected component. **CVE ID: CVE-2025-1644**	N/A	A-MOD-MODE-040325/100
Vendor: monospace					
Product: directus					
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.1.2					
Incorrect Authorization	19-Feb-2025	5.4	Directus is a real-time API and App dashboard for managing SQL database content. In affected versions if there are two overlapping policies for the `update` action that allow access to different fields, instead of correctly checking access permissions against the item they apply for the user is allowed to update the superset of fields allowed by any of the policies. E.g. have one policy allowing update access to `field_a` if the `id == 1` and one policy allowing update access to `field_b` if the `id == 2`. The user with both these policies is allowed to update both `field_a` and `field_b` for the items with ids `1` and `2`. Before v11, if a user was allowed to update an item they were allowed to update the fields that the single permission, that	https://github.com/directus/directus/security/advisories/GHSA-99vm-5v2h-h6r6	A-MON-DIRE-040325/101

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
			applied to that item, listed. With overlapping permissions this isn't as clear cut anymore and the union of fields might not be the fields the user is allowed to update for that specific item. The solution that this PR introduces is to evaluate the permissions for each field that the user tries to update in the validateItemAccess DB query, instead of only verifying access to the item as a whole. This is done by, instead of returning the actual field value, returning a flag that indicates if the user has access to that field. This uses the same case/when mechanism that is used for stripping out non permitted field that is at the core of the permissions engine. As a result, for every item that the access is validated for, the expected result is an item that has either 1 or null for all the "requested" fields instead of any of the actual field values. These results are not useful for anything other than verifying the field level access permissions. The final check in validateItemAccess can either fail if the number of items does not match the number of items the access is checked for (ie. the user does not have access to the item at all) or if not all of the passed in fields have access permissions for any of the returned items. This is a vulnerability that allows update access to unintended fields, potentially impacting the password field for user		

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
			accounts. This has been addressed in version 11.1.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-27089**		
Vendor: mrlegend1235					
Product: typed_js					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Typed JS: A typewriter style animation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'typespeed' parameter in all versions up to, and including, 1.2.0 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-2025-1328**	N/A	A-MRL-TYPE-040325/102
Vendor: navidrome					
Product: navidrome					
Affected Version(s): From (including) 0.52.0 Up to (excluding) 0.54.5					
Improper Authentication	24-Feb-2025	6.5	Navidrome is an open source web-based music collection server and streamer. Starting in version 0.52.0 and prior to version 0.54.5, in certain Subsonic API endpoints, a flaw in the authentication check process allows an attacker to specify any arbitrary username that does not exist on the system, along with a salted hash of an empty password. Under these conditions,	https://github.com/navidrome/navidrome/commit/287079a9e409fb6b9708ca384d7daa7b5185c1a0, https://github.com/navidrome/navidrome/security/advisories/GHSA-c3p4-vm8f-386p	A-NAV-NAVI-040325/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Navidrome treats the request as authenticated, granting access to various Subsonic endpoints without requiring valid credentials. An attacker can use any non-existent username to bypass the authentication system and gain access to various read-only data in Navidrome, such as user playlists. However, any attempt to modify data fails with a "permission denied" error due to insufficient permissions, limiting the impact to unauthorized viewing of information. Version 0.54.5 contains a patch for this issue. **CVE ID: CVE-2025-27112**		
Vendor: Ncrafts					
Product: formcraft					
Affected Version(s): * Up to (excluding) 3.9.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	7.2	The FormCraft plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.9.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. **CVE ID: CVE-2025-0817**	N/A	A-NCR-FORM-040325/104
Missing Authorization	18-Feb-2025	4.3	The FormCraft plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check in formcraft-main.php in all versions up to, and including, 3.9.11. This makes it possible for	N/A	A-NCR-FORM-040325/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attackers, with Subscriber-level access and above, to export all plugin data which may contain sensitive information from form submissions. **CVE ID: CVE-2024-13783**		
Vendor: needyamin					
Product: library_card_system					
Affected Version(s): 1.0					
Improper Access Control	16-Feb-2025	7.3	A vulnerability was found in needyamin Library Card System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /signup.php of the component Add Picture. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1355**	N/A	A-NEE-LIBR-040325/106
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Feb-2025	6.3	A vulnerability was found in needyamin Library Card System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file card.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1356**	N/A	A-NEE-LIBR-040325/107

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
Vendor: nilambar					
Product: prime_addons_for_elementor					
Affected Version(s): * Up to (including) 2.0.1					
Improper Access Control	20-Feb-2025	4.3	The Prime Addons for Elementor plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.0.1 via the pae_global_block shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract information from posts that are not public, including drafts, private, password protected, and restricted posts. This applies to posts created with Elementor only. **CVE ID: CVE-2024-13855**	N/A	A-NIL-PRIM-040325/108
Vendor: Odoo					
Product: odoo					
Affected Version(s): 15.0					
Improper Access Control	25-Feb-2025	8.1	Improper access control in the auth_oauth module of Odoo Community 15.0 and Odoo Enterprise 15.0 allows an internal user to export the OAuth tokens of other users. **CVE ID: CVE-2024-12368**	N/A	A-ODO-ODOO-040325/109
Affected Version(s): 17.0					
Improper Access Control	25-Feb-2025	7.5	Improper access control in mail module of Odoo Community 17.0 and Odoo Enterprise 17.0 allows remote authenticated attackers to extract sensitive information via an oracle-based (yes/no response) crafted attack.	N/A	A-ODO-ODOO-040325/110

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
			CVE ID: CVE-2024-36259		
Vendor: oliverfriedmann					
Product: ziggeo					
Affected Version(s): * Up to (excluding) 3.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The Ziggeo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ziggeo_event' shortcode in all versions up to, and including, 3.1 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-2024-12452**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3242184%40ziggeo&new=3242184%40ziggeo&sfp_email=&sfph_mail=	A-OLI-ZIGG-040325/111
Vendor: patternsinthecloud					
Product: autoship_cloud					
Affected Version(s): * Up to (excluding) 2.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The Autoship Cloud for WooCommerce Subscription Products plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'autoship-create-scheduled-order-action' shortcode in all versions up to, and including, 2.8.0 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	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3242136%40autoship-cloud&new=3242136%40autoship-cloud&sfp_email=&sfph_mail=	A-PAT-AUTO-040325/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an injected page. **CVE ID: CVE-2024-13461**		
Vendor: photonicgnostic					
Product: library_bookshelves					
Affected Version(s): * Up to (including) 5.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Library Bookshelves plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bookshelf' shortcode in all versions up to, and including, 5.9 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-2024-13464**	N/A	A-PHO-LIBR-040325/113
Vendor: phpgurukul					
Product: online_nurse_hiring_system					
Affected Version(s): 1.0					
Relative Path Traversal	23-Feb-2025	6.5	A vulnerability has been found in PHPGurukul Online Nurse Hiring System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/manage-nurse.php. The manipulation of the argument profilepic leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting vulnerability classes. **CVE ID: CVE-2025-1588**	N/A	A-PHP-ONLI-040325/114

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 Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Feb-2025	6.3	A vulnerability classified as critical has been found in PHPGurukul Online Nurse Hiring System 1.0. This affects an unknown part of the file /admin/search-report-details.php. The manipulation of the argument searchinput leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1583**	N/A	A-PHP-ONLI-040325/115
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Feb-2025	6.3	A vulnerability was found in PHPGurukul Online Nurse Hiring System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/all-request.php. The manipulation of the argument viewid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1582**	N/A	A-PHP-ONLI-040325/116
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Feb-2025	6.3	A vulnerability was found in PHPGurukul Online Nurse Hiring System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /book-nurse.php?bookid=1. The manipulation of the argument contactname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1581**	N/A	A-PHP-ONLI-040325/117
Product: online_shopping_portal					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Feb-2025	6.3	A vulnerability, which was classified as critical, was found in PHPGurukul Online Shopping Portal 2.1. This affects an unknown part of the file /search-result.php. The manipulation of the argument product leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1578**	N/A	A-PHP-ONLI-040325/118
Vendor: Phusion					
Product: passenger					
Affected Version(s): From (including) 6.0.21 Up to (excluding) 6.0.26					
Use of Uninitialized Resource	24-Feb-2025	5.3	The http parser in Phusion Passenger 6.0.21 through 6.0.25 before 6.0.26 allows a denial of service during parsing of a request with an invalid HTTP method. **CVE ID: CVE-2025-26803**	https://blog.phusion.nl/2025/02/19/passenger-6-0-26/, https://github.com/phusion/passenger/commit/bb15591646687064ab2d578d5f9660b2a4168017, https://github.com/phusion/passenger/compare/release-6.0.25...release-6.0.26	A-PHU-PASS-040325/119
Vendor: pinpoint					
Product: pinpoint_booking_system					
Affected Version(s): * Up to (including) 2.9.9.5.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	21-Feb-2025	6.5	The Pinpoint Booking System – #1 WordPress Booking Plugin plugin for WordPress is vulnerable to SQL Injection via the 'language' parameter in all versions up to, and including, 2.9.9.5.2 due to	https://plugins.trac.wordpress.org/browser/booking-system/trunk/includes/translation/class-backend-	A-PIN-PINP-040325/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			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 Subscriber-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-2024-13235**	translation.php#L125	
Vendor: pixelgrade					
Product: open_hours					
Affected Version(s): * Up to (including) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Open Hours – Easy Opening Hours plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'open-hours-current-status' shortcode in all versions up to, and including, 1.0.9 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-2024-12813**	N/A	A-PIX-OPEN-040325/121
Vendor: pixelite					
Product: events_manager					
Affected Version(s): * Up to (excluding) 6.6.4					
Improper Neutralization of Special Elements used in an	21-Feb-2025	7.5	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to time-based SQL Injection	N/A	A-PIX-EVEN-040325/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			via the active_status parameter in all versions up to, and including, 6.6.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-11260**		
Vendor: platcom					
Product: wp-asambleas					
Affected Version(s): * Up to (including) 2.85.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The WP-Asambleas plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'polls_popup' shortcode in all versions up to, and including, 2.85.0 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-2024-13579**	N/A	A-PLA-WP-A-040325/123
Vendor: pluginus					
Product: active_products_tables_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.0.6.7					
Improper Neutralization of Input During Web	18-Feb-2025	6.1	The Active Products Tables for WooCommerce. Use constructor to create tables plugin for WordPress is	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_	A-PLU-ACTI-040325/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			vulnerable to Reflected Cross-Site Scripting via the 'shortcodes_set' parameter in all versions up to, and including, 1.0.6.6 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-2025-0864**	mail=&reponame=&old=3235888%40profit-products-tables-for-woocommerce&new=3235888%40profit-products-tables-for-woocommerce&sfp_email=&sfph_mail=	
Vendor: presslayouts					
Product: pressmart					
Affected Version(s): * Up to (excluding) 1.2.17					
Improper Control of Generation of Code ('Code Injection')	18-Feb-2025	7.3	The PressMart - Modern Elementor WooCommerce WordPress Theme theme for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.2.16. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes. **CVE ID: CVE-2024-13797**	N/A	A-PRE-PRES-040325/125
Vendor: radiustheme					
Product: classified_listing					
Affected Version(s): * Up to (excluding) 4.0.5					
Exposure of Sensitive Information to an Unauthorize	25-Feb-2025	5.3	The Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to Sensitive Information	https://plugins.trac.wordpress.org/changeset/3241883/classified-listing	A-RAD-CLAS-040325/126

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
d Actor			Exposure in all versions up to, and including, 4.0.4 via the rtcl_taxonomy_settings_export function. This makes it possible for unauthenticated attackers to extract sensitive data including API keys and tokens. **CVE ID: CVE-2025-1063**		
Vendor: raptive					
Product: raptive_ads					
Affected Version(s): * Up to (including) 3.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Feb-2025	6.1	The Raptive Ads plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'poc' parameter in all versions up to, and including, 3.6.3 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-2024-13363**	N/A	A-RAP-RAPT-040325/127
Missing Authorization	19-Feb-2025	5.3	The Raptive Ads plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the site_ads_files_reset() and cls_file_reset() functions in all versions up to, and including, 3.6.3. This makes it possible for unauthenticated attackers to reset the ad and cls files. **CVE ID: CVE-2024-13364**	N/A	A-RAP-RAPT-040325/128
Vendor: razormist					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: employee_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2025	2.4	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /department.php of the component Department Page. The manipulation of the argument Department Name leads to cross site scripting. The attack can be launched remotely. **CVE ID: CVE-2025-1591**	N/A	A-RAZ-EMPL-040325/129
Vendor: royal-elementor-addons					
Product: royal_elementor_addons					
Affected Version(s): * Up to (including) 1.7.1007					
Cross-Site Request Forgery (CSRF)	19-Feb-2025	6.1	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.7.1007. This is due to missing or incorrect nonce validation on the 'wpr_filter_woo_products' function. This makes it possible for unauthenticated attackers to inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2025-1441**	N/A	A-ROY-ROYA-040325/130
Vendor: ryansolid					
Product: dom_expressions					
Affected Version(s): * Up to (excluding) 0.39.5					
Improper Neutralizati	21-Feb-2025	7.3	dom-expressions is a Fine-Grained Runtime for	https://github.com/ryansolid/d	A-RYA-DOM_-040325/131

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
on of Input During Web Page Generation ('Cross-site Scripting')			Performant DOM Rendering. In affected versions the use of javascript's `.replace()` opens up to potential Cross-site Scripting (XSS) vulnerabilities with the special replacement patterns beginning with `$`. Particularly, when the attributes of `Meta` tag from solid-meta are user-defined, attackers can utilise the special replacement patterns, either `$'` or `$\`` to achieve XSS. The solid-meta package has this issue since it uses `useAffect` and context providers, which injects the used assets in the html header. "dom-expressions" uses `.replace()` to insert the assets, which is vulnerable to the special replacement patterns listed above. This effectively means that if the attributes of an asset tag contained user-controlled data, it would be vulnerable to XSS. For instance, there might be meta tags for the open graph protocol in a user profile page, but if attackers set the user query to some payload abusing `.replace()`, then they could execute arbitrary javascript in the victim's web browser. Moreover, it could be stored and cause more problems. This issue has been addressed in version 0.39.5 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-27108**	om-expressions/commit/521f75dfa89ed24161646e7007d9d7d21da07767, https://github.com/ryansolid/dom-expressions/security/advisories/GHSA-hw62-58pr-7wc5	
Vendor: satollo					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: head\,_footer\,_and_post_injections					
Affected Version(s): * Up to (excluding) 3.3.1					
Improper Control of Generation of Code ('Code Injection')	21-Feb-2025	4.1	The Head, Footer and Post Injections plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 3.3.0. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject PHP Code in multisite environments. **CVE ID: CVE-2024-13900**	https://plugins.trac.wordpress.org/changeset/3244016/	A-SAT-HEAD-040325/132
Vendor: seacms					
Product: seacms					
Affected Version(s): * Up to (including) 13.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Feb-2025	9.8	Seacms <=13.3 is vulnerable to SQL Injection in admin_members.php. **CVE ID: CVE-2025-25513**	N/A	A-SEA-SEAC-040325/133
Vendor: shaonback2					
Product: simple_map_no_api					
Affected Version(s): * Up to (including) 1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Simple Map No Api plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter in all versions up to, and including, 1.9 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.	N/A	A-SHA-SIMP-040325/134

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
			CVE ID: CVE-2024-13565		
Vendor: shenyanzhi					
Product: memorialday					
Affected Version(s): * Up to (excluding) 1.1.0					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	6.1	The MemorialDay plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.4. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13523**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3232363%40memorialday%2Ftrunk&old=3207291%40memorialday%2Ftrunk&sfp_email=&sfph_mail=	A-SHE-MEMO-040325/135
Vendor: shopwarden					
Product: shopwarden					
Affected Version(s): * Up to (excluding) 1.0.12					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	8.8	The Shopwarden – Automated WooCommerce monitoring & testing plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.11. This is due to missing or incorrect nonce validation on the save_setting() function. This makes it possible for unauthenticated attackers to update arbitrary options and achieve privilege escalation via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3238978%40shopwarden&new=3238978%40shopwarden&sfp_email=&sfph_mail=	A-SHO-SHOP-040325/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-13315		
Vendor: simplebooklet					
Product: simplebooklet					
Affected Version(s): * Up to (excluding) 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Simplebooklet PDF Viewer and Embedder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'simplebooklet' shortcode in all versions up to, and including, 1.1.0 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-2024-13588**	N/A	A-SIM-SIMP-040325/137
Vendor: smartzminds					
Product: reset					
Affected Version(s): * Up to (including) 1.6					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	8.1	The Reset plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6. This is due to missing or incorrect nonce validation on the reset_db_page() function. This makes it possible for unauthenticated attackers to reset several tables in the database like comments, themes, plugins, and more via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	N/A	A-SMA-RESE-040325/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-13684		
Vendor: softdiscover					
Product: zigaform					
Affected Version(s): * Up to (excluding) 7.4.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Zigaform – Price Calculator & Cost Estimation Form Builder Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zgfm_fvar' shortcode in all versions up to, and including, 7.4.2 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-2024-13587**	N/A	A-SOF-ZIGA-040325/139
Affected Version(s): * Up to (including) 7.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Zigaform – Form Builder Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zgfm_rfvar' shortcode in all versions up to, and including, 7.4.2 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-2024-13573**	N/A	A-SOF-ZIGA-040325/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: speedsize					
Product: speedsize_image_\&_video_ai-optimizer					
Affected Version(s): * Up to (excluding) 1.5.2					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	4.3	The SpeedSize Image & Video AI-Optimizer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.1. This is due to missing or incorrect nonce validation on the 'speedsize_clear_css_cache_action' function. This makes it possible for unauthenticated attackers to clear the plugins cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13438**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3236368%40speedsize-ai-image-optimizer&new=3236368%40speedsize-ai-image-optimizer&sfp_email=&sfph_mail=	A-SPE-SPEE-040325/141
Vendor: supporthost					
Product: simple_charts					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Simple Charts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'simple_chart' shortcode in all versions up to, and including, 1.0 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-2024-13581**	N/A	A-SUP-SIMP-040325/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: tawk					
Product: tawk.to					
Affected Version(s): * Up to (including) 1.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2025	6.1	TawkTo Widget Version <= 1.3.7 is vulnerable to Cross Site Scripting (XSS) due to processing user input in a way that allows JavaScript execution. **CVE ID: CVE-2024-57026**	N/A	A-TAW-TAWK-040325/143
Vendor: tchgdns					
Product: wp-appbox					
Affected Version(s): * Up to (excluding) 4.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The WP-Appbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's appbox shortcode in all versions up to, and including, 4.5.4 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-2025-1489**	https://plugins.trac.wordpress.org/changeset/3244084/	A-TCH-WP-A-040325/144
Vendor: tcoderbd					
Product: tcbd_tooltip					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The TCBD Tooltip plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tcbdtooltip_text' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied	N/A	A-TCO-TCBD-040325/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2024-13388**		
Vendor: the-guild					
Product: graphql_mesh					
Affected Version(s): 0.96.5					
Uncontrolled Resource Consumption	20-Feb-2025	7.5	GraphQL Mesh is a GraphQL Federation framework and gateway for both GraphQL Federation and non-GraphQL Federation subgraphs, non-GraphQL services, such as REST and gRPC, and also databases such as MongoDB, MySQL, and PostgreSQL. When a user transforms on the root level or single source with transforms, and the client sends the same query with different variables, the initial variables are used in all following requests until the cache evicts DocumentNode. If a token is sent via variables, the following requests will act like the same token is sent even if the following requests have different tokens. This can cause a short memory leak but it won't grow per each request but per different operation until the cache evicts DocumentNode by LRU mechanism. **CVE ID: CVE-2025-27097**	https://github.com/ardatan/graphql-mesh/security/advisories/GHSA-rr4x-crhf-8886	A-THE-GRAP-040325/146
Affected Version(s): 0.96.6					
Uncontrolled Resource	20-Feb-2025	7.5	GraphQL Mesh is a GraphQL Federation framework and	https://github.com/ardatan/gra	A-THE-GRAP-040325/147

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
Consumption			gateway for both GraphQL Federation and non-GraphQL Federation subgraphs, non-GraphQL services, such as REST and gRPC, and also databases such as MongoDB, MySQL, and PostgreSQL. When a user transforms on the root level or single source with transforms, and the client sends the same query with different variables, the initial variables are used in all following requests until the cache evicts DocumentNode. If a token is sent via variables, the following requests will act like the same token is sent even if the following requests have different tokens. This can cause a short memory leak but it won't grow per each request but per different operation until the cache evicts DocumentNode by LRU mechanism. **CVE ID: CVE-2025-27097**	phql-mesh/security/advisories/GHSA-rr4x-crhf-8886	
Affected Version(s): 0.96.7					
Uncontrolled Resource Consumption	20-Feb-2025	7.5	GraphQL Mesh is a GraphQL Federation framework and gateway for both GraphQL Federation and non-GraphQL Federation subgraphs, non-GraphQL services, such as REST and gRPC, and also databases such as MongoDB, MySQL, and PostgreSQL. When a user transforms on the root level or single source with transforms, and the client sends the same query with different variables, the initial variables are used in all following requests until the cache evicts DocumentNode. If a token is	https://github.com/ardatan/graphql-mesh/security/advisories/GHSA-rr4x-crhf-8886	A-THE-GRAP-040325/148

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
			sent via variables, the following requests will act like the same token is sent even if the following requests have different tokens. This can cause a short memory leak but it won't grow per each request but per different operation until the cache evicts DocumentNode by LRU mechanism. **CVE ID: CVE-2025-27097**		
Affected Version(s): 0.96.8					
Uncontrolled Resource Consumption	20-Feb-2025	7.5	GraphQL Mesh is a GraphQL Federation framework and gateway for both GraphQL Federation and non-GraphQL Federation subgraphs, non-GraphQL services, such as REST and gRPC, and also databases such as MongoDB, MySQL, and PostgreSQL. When a user transforms on the root level or single source with transforms, and the client sends the same query with different variables, the initial variables are used in all following requests until the cache evicts DocumentNode. If a token is sent via variables, the following requests will act like the same token is sent even if the following requests have different tokens. This can cause a short memory leak but it won't grow per each request but per different operation until the cache evicts DocumentNode by LRU mechanism. **CVE ID: CVE-2025-27097**	https://github.com/ardatan/graphql-mesh/security/advisories/GHSA-rr4x-crhf-8886	A-THE-GRAP-040325/149
Product: graphql_mesh_cli					
Affected Version(s): From (including) 0.78.0 Up to (excluding) 0.82.22					

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Feb-2025	5.8	GraphQL Mesh is a GraphQL Federation framework and gateway for both GraphQL Federation and non-GraphQL Federation subgraphs, non-GraphQL services, such as REST and gRPC, and also databases such as MongoDB, MySQL, and PostgreSQL. Missing check vulnerability in the static file handler allows any client to access the files in the server's file system. When `staticFiles` is set in the `serve` settings in the configuration file, the following handler doesn't check if `absolutePath` is still under the directory provided as `staticFiles`. Users have two options to fix vulnerability; 1. Update `@graphql-mesh/cli` to a version higher than `0.82.21`, and if you use `@graphql-mesh/http`, update it to a version higher than `0.3.18` 2. Remove `staticFiles` option from the configuration, and use other solutions to serve static files. **CVE ID: CVE-2025-27098**	https://github.com/ardatan/graphql-mesh/security/advisories/GHSA-j2wh-wrv3-4x4g	A-THE-GRAP-040325/150
Product: graphql_mesh_http					
Affected Version(s): * Up to (excluding) 0.3.19					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Feb-2025	5.8	GraphQL Mesh is a GraphQL Federation framework and gateway for both GraphQL Federation and non-GraphQL Federation subgraphs, non-GraphQL services, such as REST and gRPC, and also databases such as MongoDB, MySQL, and PostgreSQL. Missing check vulnerability in the static file handler allows any client to access the files	https://github.com/ardatan/graphql-mesh/security/advisories/GHSA-j2wh-wrv3-4x4g	A-THE-GRAP-040325/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the server's file system. When `staticFiles` is set in the `serve` settings in the configuration file, the following handler doesn't check if `absolutePath` is still under the directory provided as `staticFiles`. Users have two options to fix vulnerability; 1. Update `@graphql-mesh/cli` to a version higher than `0.82.21`, and if you use `@graphql-mesh/http`, update it to a version higher than `0.3.18` 2. Remove `staticFiles` option from the configuration, and use other solutions to serve static files. **CVE ID: CVE-2025-27098**		
Vendor: Theeventscalendar					
Product: event_tickets					
Affected Version(s): * Up to (excluding) 5.19.1.2					
Missing Authorization	21-Feb-2025	5.3	The Event Tickets and Registration plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'ajax_ticket_delete' function in all versions up to, and including, 5.19.1.1. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary Attendee tickets. **CVE ID: CVE-2025-1402**	N/A	A-THE-EVEN-040325/152
Vendor: themepoints					
Product: super_testimonials					
Affected Version(s): * Up to (excluding) 4.0.2					
Improper Neutralization of Script-Related	18-Feb-2025	7.2	The Super Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_	A-THE-SUPE-040325/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
HTML Tags in a Web Page (Basic XSS)			'st_user_title' parameter in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13704**	mail=&reponame=&old=3240039%40super-testimonial&new=3240039%40super-testimonial&sfp_email=&sfph_mail=	
Vendor: Trustwave					
Product: modsecurity					
Affected Version(s): 3.0.13					
Encoding Error	25-Feb-2025	7.5	Libmodsecurity is one component of the ModSecurity v3 project. The library codebase serves as an interface to ModSecurity Connectors taking in web traffic and applying traditional ModSecurity processing. A bug that exists only in Libmodsecurity3 version 3.0.13 means that, in 3.0.13, Libmodsecurity3 can't decode encoded HTML entities if they contains leading zeroes. Version 3.0.14 contains a fix. No known workarounds are available. **CVE ID: CVE-2025-27110**	https://github.com/owasp-modsecurity/ModSecurity/security/advisories/GHSA-42w7-rmv5-4x2j	A-TRU-MODS-040325/154
Vendor: tusharimran					
Product: ablocks					
Affected Version(s): * Up to (excluding) 1.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The aBlocks – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the "Table Of Content" Block, specifically in the "markerView" attribute, in all versions up to, and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3236611%40ablocks&new=3236611%4	A-TUS-ABLO-040325/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 1.6.1 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-2024-13465**	0ablocks&sfp_email=&sfph_mail=	
Vendor: ultimatemember					
Product: ultimate_member					
Affected Version(s): * Up to (excluding) 2.10.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2025	5.3	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to second-order SQL Injection via filenames in all versions up to, and including, 2.9.2 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 access to upload files and manage filenames through a third-party plugin like a File Manager, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The risk of this vulnerability is very minimal as it requires a user to be able to manipulate filenames in order to successfully exploit. **CVE ID: CVE-2024-12276**	https://plugins.trac.wordpress.org/changeset/3242743/ultimate-member/tags/2.10.0/includes/core/class-uploader.php	A-ULT-ULTI-040325/156

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
Vendor: undsgn					
Product: uncode					
Affected Version(s): * Up to (excluding) 2.9.1.7					
Improper Input Validation	18-Feb-2025	7.5	The Uncode theme for WordPress is vulnerable to arbitrary file read due to insufficient input validation in the 'uncode_admin_get_oembed' function in all versions up to, and including, 2.9.1.6. This makes it possible for unauthenticated attackers to read arbitrary files on the server. **CVE ID: CVE-2024-13681**	N/A	A-UND-UNCO-040325/157
Improper Input Validation	18-Feb-2025	6.5	The Uncode theme for WordPress is vulnerable to arbitrary file read due to insufficient input validation in the 'uncode_recordMedia' function in all versions up to, and including, 2.9.1.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary files on the server. **CVE ID: CVE-2024-13691**	N/A	A-UND-UNCO-040325/158
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	5.4	The Uncode theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mle-description' parameter in all versions up to, and including, 2.9.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13667**	N/A	A-UND-UNCO-040325/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: unlimited-elements					
Product: unlimited_elements_for_elementor					
Affected Version(s): * Up to (excluding) 1.5.141					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Transparent Split Hero widget in all versions up to, and including, 1.5.140 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. Note: Since the widget code isn't part of the code base, to apply the patch, the affected widget: Transparent Split Hero must be deleted and reinstalled manually. **CVE ID: CVE-2024-13155**	N/A	A-UNL-UNLI-040325/160
Vendor: vanderwijk					
Product: content_blocks					
Affected Version(s): * Up to (excluding) 3.3.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Content Blocks (Custom Post Widget) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘content’ parameter within the plugin's shortcode Content Block in all versions up to, and including, 3.3.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to	https://plugins.trac.wordpress.org/changeset/3146407/#file6, https://plugins.trac.wordpress.org/changeset/3147521/	A-VAN-CONT-040325/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-6432**		
Vendor: vcita					
Product: online_payments_-_get_paid_with_paypal\,_square_\&_stripe					
Affected Version(s): * Up to (excluding) 3.30.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Online Payments – Get Paid with PayPal, Square & Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 3.20.0 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-2024-11895**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3241650%40paypal-payment-button-by-vcita&new=3241650%40paypal-payment-button-by-vcita&sfp_email=&sfph_mail=	A-VCI-ONLI-040325/162
Vendor: victorfreitas					
Product: wpupper_share_buttons					
Affected Version(s): * Up to (including) 3.51					
Cross-Site Request Forgery (CSRF)	21-Feb-2025	4.3	The WPUpper Share Buttons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.51. This is due to missing or incorrect nonce validation on the 'save_custom_css_request' function. This makes it possible for unauthenticated attackers to inject custom CSS to modify a site via a forged request granted they can	N/A	A-VIC-WPUP-040325/163

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
			trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13883**		
Vendor: webcodingplace					
Product: ultimate_classified_listings					
Affected Version(s): * Up to (excluding) 1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	4.4	The Ultimate Classified Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Title parameter in all versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID: CVE-2024-13748**	N/A	A-WEB-ULTI-040325/164
Affected Version(s): * Up to (including) 1.4					
Cross-Site Request Forgery (CSRF)	20-Feb-2025	8.1	The Ultimate Classified Listings plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or incorrect nonce validation on the update_profile function. This makes it possible for unauthenticated attackers to modify victim's email via a forged request, which might lead to account takeover, granted they can trick a user into performing	https://plugins.trac.wordpress.org/browser/ultimate-classified-listings/tags/1.4/classes/class-shortcodes.php#L701	A-WEB-ULTI-040325/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an action such as clicking on a link. **CVE ID: CVE-2024-13753**		
Vendor: webdevocean					
Product: 3d_photo_gallery					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2025	6.4	The 3D Photo Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'des[]' parameter in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13751**	N/A	A-WEB-3D_P-040325/166
Product: pricing_tables					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	6.4	The Simple Pricing Tables For WPBakery Page Builder(Formerly Visual Composer) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wdo_simple_pricing_table_free' shortcode in all versions up to, and including, 1.0 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	N/A	A-WEB-PRIC-040325/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an injected page. **CVE ID: CVE-2024-13582**		
Product: team_builder					
Affected Version(s): * Up to (including) 1.3					
Missing Authorization	18-Feb-2025	4.3	The Team Builder – Meet the Team plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_team_builder_options() function in all versions up to, and including, 1.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings. **CVE ID: CVE-2024-13687**	N/A	A-WEB-TEAM-040325/168
Vendor: webfactoryltd					
Product: advanced_google_recaptcha					
Affected Version(s): * Up to (excluding) 1.2.8					
Guessable CAPTCHA	25-Feb-2025	5.3	The Advanced Google reCaptcha plugin for WordPress is vulnerable to CAPTCHA Bypass in versions up to, and including, 1.27 . This makes it possible for unauthenticated attackers to bypass the Built-in Math Captcha Verification. **CVE ID: CVE-2025-1262**	https://plugins.trac.wordpress.org/changeset/3244677/advanced-google-recaptcha	A-WEB-ADVA-040325/169
Vendor: wecantrack					
Product: affiliate_links					
Affected Version(s): * Up to (excluding) 3.1.0					
Missing Authorization	18-Feb-2025	8.1	The Affiliate Links: WordPress Plugin for Link Cloaking and Link Management plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3238736%40affiliate-	A-WEC-AFFI-040325/170

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
			including, 3.0.1 via deserialization of untrusted input from an file export. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. **CVE ID: CVE-2024-13556**	links&new=3238736%40affiliate-links&sfp_email=&sfph_mail=	
Vendor: wegia					
Product: wegia					
Affected Version(s): * Up to (excluding) 3.2.13					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `informacao_adicional.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26606**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-rxjr-cw9q-cwwg	A-WEG-WEGI-040325/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `documento_excluir.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26607**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-g6wj-3vm2-c59m	A-WEG-WEGI-040325/172
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `dependente_docdependente.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26608**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-65h2-7484-2pww	A-WEG-WEGI-040325/173
Improper Neutralization of Special Elements used in an	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-h7jx-	A-WEG-WEGI-040325/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			vulnerability was discovered in the WeGIA application, `familiar_docfamiliar.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26609**	ggv8-v2rh	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `restaurar_produto_desocultar.php` endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26610**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-6p7c-9hcx-jpqj	A-WEG-WEGI-040325/175
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `remover_produto.php` endpoint. This vulnerability	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-q273-4vcj-qqp4	A-WEG-WEGI-040325/176

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
			could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26611**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `adicionar_almoxarife.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26612**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-9cwj-p4x6-pp88	A-WEG-WEGI-040325/177
Affected Version(s): * Up to (excluding) 3.2.14					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. An OS Command Injection vulnerability was discovered in the WeGIA application, `gerenciar_backup.php` endpoint. This vulnerability could allow an attacker to execute arbitrary code remotely. This issue has been addressed in version	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-g3w6-m6w8-p6r2	A-WEG-WEGI-040325/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26613**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2025	9.8	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `historico_paciente.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26617**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-f654-c5r5-jx77	A-WEG-WEGI-040325/179
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Feb-2025	9.8	WeGIA is a Web Manager for Institutions with a focus on Portuguese language. A SQL Injection vulnerability was discovered in the WeGIA application, personalizacao_upload.php endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-27096**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-j856-wh9m-9vpm	A-WEG-WEGI-040325/180
Improper Neutralizati	18-Feb-2025	8.8	WeGIA is an open source Web Manager for	https://github.com/LabRedesCe	A-WEG-WEGI-040325/181

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
on of Special Elements used in an SQL Command ('SQL Injection')			Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `deletar_documento.php` endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26614**	fetRJ/WeGIA/security/advisories/GHSA-3qhx-gfqj-vm2j	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Feb-2025	7.5	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Path Traversal vulnerability was discovered in the WeGIA application, `exportar_dump.php` endpoint. This vulnerability could allow an attacker to gain unauthorized access to sensitive information stored in `config.php`. `config.php` contains information that could allow direct access to the database. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26616**	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-xxqg-p22h-3f32	A-WEG-WEGI-040325/182
Improper Limitation of a Pathname to a Restricted Directory ('Path	18-Feb-2025	10	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Path Traversal vulnerability was discovered in the WeGIA	https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-p5wx-pv8j-f96h	A-WEG-WEGI-040325/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Traversal')			application, `examples.php` endpoint. This vulnerability could allow an attacker to gain unauthorized access to sensitive information stored in `config.php`. `config.php` contains information that could allow direct access to the database. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID: CVE-2025-26615**		
Affected Version(s): * Up to (excluding) 3.2.15					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Feb-2025	9.8	WeGIA is a Web manager for charitable institutions. An OS Command Injection vulnerability was discovered in versions prior to 3.2.15 of the WeGIA application, `importar_dump.php` endpoint. This vulnerability could allow an attacker to execute arbitrary code remotely. The command is basically a command to move a temporary file, so a webshell upload is also possible. Version 3.2.15 contains a patch for the issue. **CVE ID: CVE-2025-27140**	https://github.com/LabRedesCefetRJ/WeGIA/commit/7d0df8c9a0b8b7d6862bbc23dc729d73e39672a1, https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-xw6w-x28r-2p5c	A-WEG-WEGI-040325/184
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Feb-2025	8.8	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was discovered in the WeGIA application prior to version 3.2.15 at the `adicionar_tipo_exame.php` endpoint. This vulnerability allows an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. Version 3.2.15 contains a patch for the	https://github.com/LabRedesCefetRJ/WeGIA/commit/619ead748e18e685459c6dc3c226e621b9ff5403, https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-xj79-w799-qjcp	A-WEG-WEGI-040325/185

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. **CVE ID: CVE-2025-27133**		
Vendor: wow-company					
Product: modal_window					
Affected Version(s): * Up to (excluding) 6.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Modal Window – create popup modal window plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'iframeBox' shortcode in all versions up to, and including, 6.1.5 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-2025-0897**	https://plugins.trac.wordpress.org/changeset/3243077/	A-WOW-MODA-040325/186
Vendor: wpdesk					
Product: flexible_wishlist_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.2.27					
Cross-Site Request Forgery (CSRF)	18-Feb-2025	4.3	The Flexible Wishlist for WooCommerce – Ecommerce Wishlist & Save for later plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.26. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to modify/update/create other user's wishlists via a forged request granted they can trick a site administrator into	https://plugins.trac.wordpress.org/changeset?old_path=flexible-wishlist/tags/1.2.26&new_path=/flexible-wishlist/tags/1.2.27&sfp_email=&sfph_mail=	A-WPD-FLEX-040325/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID: CVE-2024-13718**		
Vendor: wpeverest					
Product: everest_forms					
Affected Version(s): * Up to (excluding) 3.0.9.5					
Unrestricted Upload of File with Dangerous Type	25-Feb-2025	9.8	The Everest Forms – Contact Forms, Quiz, Survey, Newsletter & Payment Form Builder for WordPress plugin for WordPress is vulnerable to arbitrary file upload, read, and deletion due to missing file type and path validation in the 'format' method of the EVF_Form_Fields_Upload class in all versions up to, and including, 3.0.9.4. This makes it possible for unauthenticated attackers to upload, read, and delete arbitrary files on the affected site's server which may make remote code execution, sensitive information disclosure, or a site takeover possible. **CVE ID: CVE-2025-1128**	https://github.com/wpeverest/everest-forms/commit/7d37858d2c614aa107b0f495fe50819a3867e7f5, https://github.com/wpeverest/everest-forms/pull/1406/files, https://plugins.trac.wordpress.org/changeset/3243663/everest-forms#file7	A-WPE-EVER-040325/188
Vendor: wpexperts					
Product: givewp_square					
Affected Version(s): * Up to (excluding) 1.3.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2025	6.5	The WPExperts Square For GiveWP plugin for WordPress is vulnerable to SQL Injection via the 'post' parameter in all versions up to, and including, 1.3.1 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,	https://plugins.trac.wordpress.org/changeset/3242658/wpexperts-square-for-give/trunk/includes/class-give-square.php	A-WPE-GIVE-040325/189

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
			with Subscriber-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-2024-13713**		
Product: post_smtp					
Affected Version(s): * Up to (excluding) 3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Feb-2025	7.2	The Post SMTP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the from and subject parameter in all versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2025-0521**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3237626%40post-smtp%2Ftrunk&old=3229076%40post-smtp%2Ftrunk&sfp_email=&sfph_mail=	A-WPE-POST-040325/190
Vendor: wpindeed					
Product: ultimate_learning_pro					
Affected Version(s): * Up to (excluding) 3.9.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2025	4.9	The Indeed Ultimate Learning Pro plugin for WordPress is vulnerable to time-based SQL Injection via the 'post_id' parameter in all versions up to, and including, 3.9 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 Administrator-level access and above, to append additional SQL queries into	N/A	A-WPI-ULTI-040325/191

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
			already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-13846**		
Vendor: wpmet					
Product: elementskit_elementor_addons					
Affected Version(s): * Up to (excluding) 3.4.1					
Improper Access Control	19-Feb-2025	5.3	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.4.0 due to a missing capability checks on the get_megamenu_content() function. This makes it possible for unauthenticated attackers to view any item created in Elementor, such as posts, pages and templates including drafts, trashed and private items. **CVE ID: CVE-2025-0968**	https://plugins.trac.wordpress.org/changeset/3237243/	A-WPM-ELEM-040325/192
Vendor: wwexgroup					
Product: ltl_freight_quotes					
Affected Version(s): * Up to (excluding) 2.3.13					
Missing Authorization	20-Feb-2025	5.3	The LTL Freight Quotes – GlobalTranz Edition plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the engtz_wd_save_dropship AJAX endpoint in all versions up to, and including, 2.3.12. This makes it possible for unauthenticated attackers to update the drop shipping settings. **CVE ID: CVE-2025-1483**	https://plugins.trac.wordpress.org/changeset/3243002/	A-WWE-LTL_-040325/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Xmlsoft					
Product: libxml2					
Affected Version(s): * Up to (excluding) 2.12.10					
NULL Pointer Dereference	18-Feb-2025	2.9	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a NULL pointer dereference in xmlPatMatch in pattern.c. **CVE ID: CVE-2025-27113**	N/A	A-XML-LIBX-040325/194
Affected Version(s): From (including) 2.13.0 Up to (excluding) 2.13.6					
NULL Pointer Dereference	18-Feb-2025	2.9	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a NULL pointer dereference in xmlPatMatch in pattern.c. **CVE ID: CVE-2025-27113**	N/A	A-XML-LIBX-040325/195
Vendor: xootix					
Product: login\/signup_popup					
Affected Version(s): * Up to (excluding) 2.8.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Feb-2025	6.4	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's xoo_el_action shortcode in all versions up to, and including, 2.8.5 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-2025-1064**	https://plugins.trac.wordpress.org/changeset/3239293/easy-login-woocommerce	A-XOO-LOGI-040325/196
Vendor: yawave					
Product: yawave					
Affected Version(s): * Up to (including) 2.9.1					
Improper	25-Feb-2025	7.5	The Yawave plugin for	N/A	A-YAW-YAWA-

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
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			WordPress is vulnerable to SQL Injection via the 'lbid' parameter in all versions up to, and including, 2.9.1 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-2025-1648**		040325/197
Vendor: yaycommerce					
Product: yaysmtp					
Affected Version(s): From (including) 2.4.9 Up to (excluding) 2.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Feb-2025	7.2	The YaySMTP and Email Logs: Amazon SES, SendGrid, Outlook, Mailgun, Brevo, Google and Any SMTP Service plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions 2.4.9 to 2.6.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note: The vulnerability has been initially patched in version 2.4.8 and was reintroduced in version 2.4.9 with the removal of the wp_kses_post() built-in WordPress sanitization function. **CVE ID: CVE-2025-0916**	https://plugins.trac.wordpress.org/changeset/3238172	A-YAY-YAYS-040325/198

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
Hardware					
Vendor: Dlink					
Product: dap-1320					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Feb-2025	8.8	A vulnerability classified as critical was found in D-Link DAP-1320 1.00. Affected by this vulnerability is the function set_ws_action of the file /dws/api/. The manipulation leads to heap-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID: CVE-2025-1538**	N/A	H-DLI-DAP--040325/199
Vendor: fiberhome					
Product: an5506-01-a					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2025	2.4	A vulnerability was found in FiberHome AN5506-01A ONU GPON RP2511. It has been rated as problematic. This issue affects some unknown processing of the file /goform/URL_filterCfg of the component URL Filtering Submenu. The manipulation of the argument url_IP leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1613**	N/A	H-FIB-AN55-040325/200
Improper	24-Feb-2025	2.4	A vulnerability classified as	N/A	H-FIB-AN55-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			problematic has been found in FiberHome AN5506-01A ONU GPON RP2511. Affected is an unknown function of the file /goform/portForwardingCfg of the component Port Forwarding Submenu. The manipulation of the argument pf_Description leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1614**		040325/201
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2025	2.4	A vulnerability classified as problematic was found in FiberHome AN5506-01A ONU GPON RP2511. Affected by this vulnerability is an unknown functionality of the component NAT Submenu. The manipulation of the argument Description leads to cross site scripting. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1615**	N/A	H-FIB-AN55-040325/202
Product: an5506-01a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Feb-2025	4.7	A vulnerability, which was classified as critical, has been found in FiberHome AN5506-01A ONU GPON RP2511. Affected by this issue is some unknown functionality of the component Diagnosis. The manipulation of the argument Destination	N/A	H-FIB-AN55-040325/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Address leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1616**		
Vendor: yitechnology					
Product: yi_car_dashcam					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	24-Feb-2025	9.8	Improper access control in the HTTP server in YI Car Dashcam v3.88 allows unrestricted file downloads, uploads, and API commands. API commands can also be made to make unauthorized modifications to the device settings, such as disabling recording, disabling sounds, factory reset. **CVE ID: CVE-2024-56897**	N/A	H-YIT-YI_C-040325/204
Operating System					
Vendor: Dlink					
Product: dap-1320_firmware					
Affected Version(s): 1.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Feb-2025	8.8	A vulnerability classified as critical was found in D-Link DAP-1320 1.00. Affected by this vulnerability is the function set_ws_action of the file /dws/api/. The manipulation leads to heap-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the	N/A	O-DLI-DAP--040325/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer. **CVE ID: CVE-2025-1538**		
Vendor: fiberhome					
Product: an5506-01-a_firmware					
Affected Version(s): rp2511					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2025	2.4	A vulnerability was found in FiberHome AN5506-01A ONU GPON RP2511. It has been rated as problematic. This issue affects some unknown processing of the file /goform/URL_filterCfg of the component URL Filtering Submenu. The manipulation of the argument url_IP leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1613**	N/A	O-FIB-AN55-040325/206
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2025	2.4	A vulnerability classified as problematic has been found in FiberHome AN5506-01A ONU GPON RP2511. Affected is an unknown function of the file /goform/portForwardingCfg of the component Port Forwarding Submenu. The manipulation of the argument pf_Description leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1614**	N/A	O-FIB-AN55-040325/207
Improper	24-Feb-2025	2.4	A vulnerability classified as	N/A	O-FIB-AN55-

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
Neutralization of Input During Web Page Generation ('Cross-site Scripting')		🟩	problematic was found in FiberHome AN5506-01A ONU GPON RP2511. Affected by this vulnerability is an unknown functionality of the component NAT Submenu. The manipulation of the argument Description leads to cross site scripting. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1615**		040325/208
Product: an5506-01a_firmware					
Affected Version(s): rp2511					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Feb-2025	4.7	A vulnerability, which was classified as critical, has been found in FiberHome AN5506-01A ONU GPON RP2511. Affected by this issue is some unknown functionality of the component Diagnosis. The manipulation of the argument Destination Address leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-1616**	N/A	O-FIB-AN55-040325/209
Vendor: yitechnology					
Product: yi_car_dashcam_firmware					
Affected Version(s): 3.88					
Unrestricted Upload of File with Dangerous Type	24-Feb-2025	9.8	Improper access control in the HTTP server in YI Car Dashcam v3.88 allows unrestricted file downloads, uploads, and API	N/A	O-YIT-YI_C-040325/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands. API commands can also be made to make unauthorized modifications to the device settings, such as disabling recording, disabling sounds, factory reset. **CVE ID: CVE-2024-56897**		
Vendor: zephyrproject					
Product: zephyr					
Affected Version(s): * Up to (including) 4.0					
Out-of-bounds Read	25-Feb-2025	8.2	A malicious or malformed DNS packet without a payload can cause an out-of-bounds read, resulting in a crash (denial of service) or an incorrect computation. **CVE ID: CVE-2025-1673**	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-jjhx-rrh4-j8mx	O-ZEP-ZEPH-040325/211
Out-of-bounds Read	25-Feb-2025	8.2	A lack of input validation allows for out of bounds reads caused by malicious or malformed packets. **CVE ID: CVE-2025-1674**	https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-x975-8pgf-qh66	O-ZEP-ZEPH-040325/212