SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 26 November 2025

Generated on 26 November 2025

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-41115	SCIM provisioning was introduced in Grafana Enterprise and Grafana Cloud in April to improve how organizations manage users and teams in Grafana by introducing automated user lifecycle management. In Grafana versions 12.x where SCIM provisioning is enabled and configured, a vulnerability in user identity handling allows a malicious or compromised SCIM client to provision a user with a numeric externalId, which in turn could allow to override internal user IDs and lead to impersonation or privilege escalation. This vulnerability applies only if all of the following conditions are met: - `enableSCIM` feature flag set to true - `user_sync_enabled` config option in the `[auth.scim]` block set to true	10.0	More Details
CVE-2025-63224	The Itel DAB Encoder (IDEnc build 25aec8d) is vulnerable to Authentication Bypass due to improper JWT validation across devices. Attackers can reuse a valid JWT token obtained from one device to authenticate and gain administrative access to any other device running the same firmware, even if the passwords and networks are different. This allows full compromise of affected devices.	10.0	More Details
CVE-2025-49752	Azure Bastion Elevation of Privilege Vulnerability	10.0	More Details
CVE-2025-65108	md-to-pdf is a CLI tool for converting Markdown files to PDF using Node.js and headless Chrome. Prior to version 5.2.5, a Markdown front-matter block that contains JavaScript delimiter causes the JS engine in gray-matter library to execute arbitrary code in the Markdown to PDF converter process of md-to-pdf library, resulting in remote code execution. This issue has been patched in version 5.2.5.	10.0	More Details

CVE-2025-54347	A Directory Traversal vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows an attacker to write arbitrary files under certain conditions.	9.9	More Details
CVE-2025-12057	The WavePlayer WordPress plugin before 3.8.0 does not have authorization in an AJAX action as well as does not validate the file to be copied locally, allowing unauthenticated users to upload arbitrary file on the server and lead to RCE	9.8	More Details
CVE-2025-10437	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eksagate Electronic Engineering and Computer Industry Trade Inc. Webpack Management System allows SQL Injection.This issue affects Webpack Management System: through 20251119.	9.8	More Details
CVE-2025-11456	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the eh_crm_new_ticket_post() function in all versions up to, and including, 3.3.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-66071	Missing Authorization vulnerability in tychesoftwares Custom Order Numbers for WooCommerce custom-order-numbers-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Custom Order Numbers for WooCommerce: from n/a through <= 1.11.0.	9.8	More Details
CVE-2025-66072	Missing Authorization vulnerability in Stiofan UsersWP userswp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UsersWP: from n/a through <= 1.2.47.	9.8	More Details
CVE-2025-11127	The Mstoreapp Mobile App WordPress plugin through 2.08 and Mstoreapp Mobile Multivendor through 9.0.1 do not properly verify users identify when using an AJAX action, allowing unauthenticated users to retrieve a valid session for arbitrary users by knowing their email address.	9.8	More Details
CVE-2025-63958	MILLENSYS Vision Tools Workspace 6.5.0.2585 exposes a sensitive configuration endpoint (/MILLENSYS/settings) that is accessible without authentication. This page leaks plaintext database credentials, file share paths, internal license server configuration, and software update parameters. An unauthenticated attacker can retrieve this information by accessing the endpoint directly, potentially leading to full system compromise. The vulnerability is due to missing access controls on a privileged administrative function.	9.8	More Details
CVE-2024-47856	In RSA Authentication Agent before 7.4.7, service paths and shortcut paths may be vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks. An adversary can place an executable in a higher-level directory of the path, and Windows will resolve that executable instead of the intended executable.	9.8	More Details
CVE-2025-6389	The Sneeit Framework plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.3 via the sneeit_articles_pagination_callback() function. This is due to the function accepting user input and then passing that through call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leveraged to inject backdoors or, for example, create new administrative user accounts.	9.8	More Details
CVE-2025-13559	The EduKart Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the 'edukart_pro_register_user_front_end' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-			

2025-61168	An issue in the cms_rest.php component of SIGB PMB v8.0.1.14 allows attackers to execute arbitrary code via unserializing an arbitrary file.	9.8	More Details
CVE-2025-13595	The CIBELES AI plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check in the 'actualizador_git.php' file in all versions up to, and including, 1.10.8. This makes it possible for unauthenticated attackers to download arbitrary GitHub repositories and overwrite plugin files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-59245	Microsoft SharePoint Online Elevation of Privilege Vulnerability	9.8	More Details
CVE-2025-64310	EPSON WebConfig and Epson Web Control for SEIKO EPSON Projector Products do not restrict excessive authentication attempts. An administrative user's password may be identified through a brute force attack.	9.8	More Details
CVE-2025-63807	An issue was discovered in weijiang1994 university-bbs (aka Blogin) in commit 9e06bab430bfc729f27b4284ba7570db3b11ce84 (2025-01-13). A weak verification code generation mechanism combined with missing rate limiting allows attackers to perform brute-force attacks on verification codes without authentication. Successful exploitation may result in account takeover via password reset or other authentication bypass methods.	9.8	More Details
CVE-2025-63213	The QVidium Opera11 device (firmware version 2.9.0-Ax4x-opera11) is vulnerable to Remote Code Execution (RCE) due to improper input validation on the /cgi-bin/net_ping.cgi endpoint. An attacker can exploit this vulnerability by sending a specially crafted GET request with a malicious parameter to inject arbitrary commands. These commands are executed with root privileges, allowing attackers to gain full control over the device. This poses a significant security risk to any device running this software.	9.8	More Details
CVE-2025-63218	The Axel Technology WOLF1MS and WOLF2MS devices (firmware versions 0.8.5 to 1.0.3) are vulnerable to Broken Access Control due to missing authentication on the /cgi-bin/gstFcgi.fcgi endpoint. Unauthenticated remote attackers can list user accounts, create new administrative users, delete users, and modify system settings, leading to full compromise of the device.	9.8	More Details
CVE-2025-63223	The Axel Technology StreamerMAX MK II devices (firmware versions 0.8.5 to 1.0.3) are vulnerable to Broken Access Control due to missing authentication on the /cgi-bin/gstFcgi.fcgi endpoint. Unauthenticated remote attackers can list user accounts, create new administrative users, delete users, and modify system settings, leading to full compromise of the device.	9.8	More Details
CVE-2025-63206	An authentication bypass issue was discovered in Dasan Switch DS2924 web based interface, firmware versions 1.01.18 and 1.02.00, allowing attackers to gain escalated privileges via storing crafted cookies in the web browser.	9.8	More Details
CVE-2025-63207	The R.V.R Elettronica TEX product (firmware TEXL-000400, Web GUI TLAN-000400) is vulnerable to broken access control due to improper authentication checks on the /_Passwd.html endpoint. An attacker can send an unauthenticated POST request to change the Admin, Operator, and User passwords, resulting in complete system compromise.	9.8	More Details
CVE-2025-63210	The Newtec Celox UHD (models: CELOXA504, CELOXA820) running firmware version celox-21.6.13 is vulnerable to an authentication bypass. An attacker can exploit this issue by modifying intercepted responses from the /celoxservice endpoint. By injecting a forged response body during the loginWithUserName flow, the attacker can gain Superuser or Operator access without providing valid credentials.	9.8	More Details
	Quark Cloud Drive v3.23.2 has a DLL Hijacking vulnerability. This vulnerability stems		

CVE-2025-63685	from the insecure loading of system libraries. Specifically, the application does not validate the path or signature of [regsvr32.exe] it loads. An attacker can place a crafted malicious DLL in the application's startup directory, which will be loaded and executed when the user launches the program.	9.8	More Details
CVE-2025-65099	Claude Code is an agentic coding tool. Prior to version 1.0.39, when running on a machine with Yarn 3.0 or above, Claude Code could have been tricked to execute code contained in a project via yarn plugins before the user accepted the startup trust dialog. Exploiting this would have required a user to start Claude Code in an untrusted directory and to be using Yarn 3.0 or above. This issue has been patched in version 1.0.39.	9.8	More Details
CVE-2025-60738	An issue in Ilevia EVE X1 Server Firmware Version v4.7.18.0.eden and before Logic Version v6.00 - 2025_07_21 and before allows a remote attacker to execute arbitrary code via the ping.php component does not perform secure filtering on IP parameters	9.8	More Details
CVE-2025-52410	Institute-of-Current-Students v1.0 contains a time-based blind SQL injection vulnerability in the mydetailsstudent.php endpoint. The `myds` GET parameter is not adequately sanitized before being used in SQL queries.	9.8	More Details
CVE-2025-64428	Dataease is an open source data visualization analysis tool. Versions prior to 2.10.17 are vulnerable to JNDI injection. A blacklist was added in the patch for version 2.10.14. However, JNDI injection remains possible via the iiop, corbaname, and iiopname schemes. The vulnerability has been fixed in version 2.10.17.	9.8	More Details
CVE-2025-63888	The read function in file thinkphp\library\think\template\driver\File.php in ThinkPHP 5.0.24 contains a remote code execution vulnerability.	9.8	More Details
CVE-2025-13597	The AI Feeds plugin for WordPress is vulnerable to arbitrary file uploads due to missing capability check in the 'actualizador_git.php' file in all versions up to, and including, 1.0.11. This makes it possible for unauthenticated attackers to download arbitrary GitHub repositories and overwrite plugin files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-60739	Cross Site Request Forgery (CSRF) vulnerability in Ilevia EVE X1 Server Firmware Version v4.7.18.0.eden and before, Logic Version v6.00 - 2025_07_21 allows a remote attacker to execute arbitrary code via the /bh_web_backend component	9.6	More Details
CVE-2025-10571	Authentication Bypass Using an Alternate Path or Channel vulnerability in ABB ABB Ability Edgenius.This issue affects ABB Ability Edgenius: 3.2.0.0, 3.2.1.1.	9.6	More Details
CVE-2025-33187	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT, where an attacker could use privileged access to gain access to SoC protected areas. A successful exploit of this vulnerability might lead to code execution, information disclosure, data tampering, denial of service, or escalation of privileges.	9.3	More Details
CVE-2025-12977	Fluent Bit in_http, in_splunk, and in_elasticsearch input plugins fail to sanitize tag_key inputs. An attacker with network access or the ability to write records into Splunk or Elasticsearch can supply tag_key values containing special characters such as newlines or ../ that are treated as valid tags. Because tags influence routing and some outputs derive filenames or contents from tags, this can allow newline injection, path traversal, forged record injection, or log misrouting, impacting data integrity and log routing.	9.1	More Details
CVE-2025-64767	hpke-js is a Hybrid Public Key Encryption (HPKE) module built on top of Web Cryptography API. Prior to version 1.7.5, the public SenderContext Seal() API has a race condition which allows for the same AEAD nonce to be re-used for multiple Seal() calls. This can lead to complete loss of Confidentiality and Integrity of the produced messages. This issue has been patched in version 1.7.5.	9.1	More Details

CVE-2025-65021	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an Insecure Direct Object Reference (IDOR) vulnerability exists in the poll finalization feature of the application. Any authenticated user can finalize a poll they do not own by manipulating the pollId parameter in the request. This allows unauthorized users to finalize other users' polls and convert them into events without proper authorization checks, potentially disrupting user workflows and causing data integrity and availability issues. This issue has been patched in version 4.5.4.	9.1	More Details
CVE-2025-63729	An issue was discovered in Syrotech SY-GPON-1110-WDONT SYRO_3.7L_3.1.02-240517 allowing attackers to exctract the SSL Private Key, CA Certificate, SSL Certificate, and Client Certificates in .pem format in firmware in etc folder.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-13547	A flaw has been found in D-Link DIR-822K and DWR-M920 1.00_20250513164613/1.1.50. This affects an unknown part of the file /boafrm/formDdns. This manipulation of the argument submit-url causes memory corruption. The attack may be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-13553	A weakness has been identified in D-Link DWR-M920 1.1.50. This affects the function sub_41C7FC of the file /boafrm/formPinManageSetup. This manipulation of the argument submit-url causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-13551	A vulnerability was identified in D-Link DIR-822K and DWR-M920 1.00_20250513164613/1.1.50. The affected element is an unknown function of the file /boafrm/formWanConfigSetup. The manipulation of the argument submit-url leads to buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-13400	A vulnerability was detected in Tenda CH22 1.0.0.1. Affected is the function formWrlExtraGet of the file /goform/WrlExtraGet. Performing manipulation of the argument chkHz results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.	8.8	More Details
CVE-2025-64064	Primakon Pi Portal 1.0.18 /api/v2/pp_users endpoint fails to adequately check user permissions before processing a PATCH request to modify the PP_SECURITY_PROFILE_ID. Because of weak access controls any low level user can use this API and change their permission to Administrator by using PP_SECURITY_PROFILE_ID=2 inside body of request and escalate privileges.	8.8	More Details
CVE-2025-13156	The Vitepos – Point of Sale (POS) for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the insert_media_attachment() function in all versions up to, and including, 3.3.0. This is due to the save_update_category_img() function accepting user-supplied file types without validation when processing category images. This makes it possible for authenticated attackers, with subscriber level access and above, to upload arbitrary files on the affected site's server which makes remote code execution possible.	8.8	More Details
CVE-2025-64655	Improper authorization in Dynamics OmniChannel SDK Storage Containers allows an unauthorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2025-	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to version 2.9.5, an authenticated SQL Injection vulnerability in the API allows any user, regardless of permission level, to execute arbitrary SQL queries. By	8.8	More

65103	manipulating the display parameter in an API request, an attacker can exfiltrate, modify, or delete any data in the database, leading to a full system compromise. This issue has been patched in version 2.9.5.		Details
CVE-2025-11087	The Zegen Core plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 2.0.1. This is due to missing nonce validation and missing file type validation in the '/custom-font-code/custom-fonts-uploads.php' file. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2025-63434	The update mechanism in Xtooltech Xtool AnyScan Android Application 4.40.40 and prior is insecure. The application downloads and extracts update packages containing executable code without performing a cryptographic integrity or authenticity check on their contents. An attacker who can control the update metadata can serve a malicious package, which the application will accept, extract, and later execute, leading to arbitrary code execution.	8.8	More Details
CVE-2025-13550	A vulnerability was determined in D-Link DIR-822K and DWR-M920 1.00_20250513164613/1.1.50. Impacted is an unknown function of the file /boafrm/formVpnConfigSetup. Executing manipulation of the argument submit-url can lead to buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2025-13552	A security flaw has been discovered in D-Link DIR-822K and DWR-M920 1.00_20250513164613/1.1.50. The impacted element is an unknown function of the file /boafrm/formWlEncrypt. The manipulation of the argument submit-url results in buffer overflow. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	8.8	More Details
CVE-2025-12970	The extract_name function in Fluent Bit in_docker input plugin copies container names into a fixed size stack buffer without validating length. An attacker who can create containers or control container names, can supply a long name that overflows the buffer, leading to process crash or arbitrary code execution.	8.8	More Details
CVE-2025-13549	A vulnerability was found in D-Link DIR-822K 1.00. This issue affects the function sub_455524 of the file /boafrm/formNtp. Performing manipulation of the argument submit-url results in buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-13445	A flaw has been found in Tenda AC21 16.03.08.16. This affects an unknown part of the file /goform/SetIpMacBind. Executing manipulation of the argument list can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-62703	Fugue is a unified interface for distributed computing that lets users execute Python, Pandas, and SQL code on Spark, Dask, and Ray with minimal rewrites. In version 0.9.2 and prior, there is a remote code execution vulnerability by pickle deserialization via FlaskRPCServer. The Fugue framework implements an RPC server system for distributed computing operations. In the core functionality of the RPC server implementation, I found that the _decode() function in fugue/rpc/flask.py directly uses cloudpickle.loads() to deserialize data without any sanitization. This creates a remote code execution vulnerability when malicious pickle data is processed by the RPC server. The vulnerability exists in the RPC communication mechanism where the client can send arbitrary serialized Python objects that will be deserialized on the server side, allowing attackers to execute arbitrary code on the victim's machine. This issue has been patched via commit 6f25326.	8.8	More Details
	Cross-Site Request Forgery (CSRF) vulnerability in the OAuth implementation of the Tuya SDK 6.5.0 for Android and iOS, affects the Tuya Smart and Smartlife mobile		

CVE-2025-56400	applications, as well as other third-party applications that integrate the SDK, allows an attacker to link their own Amazon Alexa account to a victim's Tuya account. The applications fail to validate the OAuth state parameter during the account linking flow, enabling a cross-site request forgery (CSRF)-like attack. By tricking the victim into clicking a crafted authorization link, an attacker can complete the OAuth flow on the victim's behalf, resulting in unauthorized Alexa access to the victim's Tuya-connected devices. This affects users regardless of prior Alexa linkage and does not require the Tuya application to be active at the time. Successful exploitation may allow remote control of devices such as cameras, doorbells, door locks, or alarms.	8.8	More Details
CVE-2025-12138	The URL Image Importer plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in all versions up to, and including, 1.0.6. This is due to the plugin relying on a user-controlled Content-Type HTTP header to validate file uploads in the 'uimptr_import_image_from_url()' function which writes the file to the server before performing proper validation. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible via the uploaded PHP file.	8.8	More Details
CVE-2025-13446	A vulnerability has been found in Tenda AC21 16.03.08.16. This vulnerability affects unknown code of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone/time leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-36072	IBM webMethods Integration 10.11 through 10.11_Core_Fix22, 10.15 through 10.15_Core_Fix22, and 11.1 through 11.1_Core_Fix6 IBM webMethods Integration allow an authenticated user to execute arbitrary code on the system, caused by the deserialization of untrusted object graphs data.	8.8	More Details
CVE-2025-13548	A vulnerability has been found in D-Link DIR-822K and DWR-M920 1.00_20250513164613/1.1.50. This vulnerability affects unknown code of the file /boafrm/formFirewallAdv. Such manipulation of the argument submit-url leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-11985	The Realty Portal plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'rp_save_property_settings' function in versions 0.1 to 0.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site. 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.	8.8	More Details
CVE-2025-62730	SOPlanning is vulnerable to Privilege Escalation in user management tab. Users with user_manage_team role are allowed to modify permissions of users. However, they are able to assign administrative permissions to any user including themselves. This allow a malicious authenticated attacker with this role to escalate to admin privileges. This issue affects both Bulk Update functionality and regular edition of user's right and privileges. This issue was fixed in version 1.55.	8.8	More Details
CVE-2025-62164	vLLM is an inference and serving engine for large language models (LLMs). From versions 0.10.2 to before 0.11.1, a memory corruption vulnerability could lead to a crash (denial-of-service) and potentially remote code execution (RCE), exists in the Completions API endpoint. When processing user-supplied prompt embeddings, the endpoint loads serialized tensors using torch.load() without sufficient validation. Due to a change introduced in PyTorch 2.8.0, sparse tensor integrity checks are disabled by default. As a result, maliciously crafted tensors can bypass internal bounds checks and trigger an out-of-bounds memory write during the call to to_dense(). This memory corruption can crash vLLM and potentially lead to code execution on the server hosting vLLM. This issue has been patched in version 0.11.1.	8.8	More Details

CVE-2025-10555	A stored Cross-site Scripting (XSS) vulnerability affecting Service Items Management in DELMIA Service Process Engineer on Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-10554	A stored Cross-site Scripting (XSS) vulnerability affecting Requirements in ENOVIA Product Manager from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-65951	Inside Track / Entropy Derby is a research-grade horse-racing betting engine. Prior to commit 2d38d2f, the VDF-based timelock encryption system fails to enforce sequential delay against the betting operator. Bettors pre-compute the entire Wesolowski VDF and include vdfOutputHex in their encrypted bet ticket, allowing the house to decrypt immediately using fast proof verification instead of expensive VDF evaluation. This issue has been patched via commit 2d38d2f.	8.7	More Details
CVE-2025-62207	Azure Monitor Elevation of Privilege Vulnerability	8.6	More Details
CVE-2025-64066	Primakon Pi Portal 1.0.18 REST /api/v2/user/register endpoint suffers from a Broken Access Control vulnerability. The endpoint fails to implement any authorization checks, allowing unauthenticated attackers to perform POST requests to register new user accounts in the application's local database. This bypasses the intended security architecture, which relies on an external Identity Provider for initial user registration and assumes that internal user creation is an administrative-only function. This vector can also be chained with other vulnerabilities for privilege escalation and complete compromise of application. This specific request can be used to also enumerate already registered user accounts, aiding in social engineering or further targeted attacks.	8.6	More Details
CVE-2025-12816	An interpretation-conflict (CWE-436) vulnerability in node-forge versions 1.3.1 and earlier enables unauthenticated attackers to craft ASN.1 structures to desynchronize schema validations, yielding a semantic divergence that may bypass downstream cryptographic verifications and security decisions.	8.6	More Details
CVE-2025-62155	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to version 0.9.6, a recently patched SSRF vulnerability contains a bypass method that can bypass the existing security fix and still allow SSRF to occur. Because the existing fix only applies security restrictions to the first URL request, a 302 redirect can bypass existing security measures and successfully access the intranet. This issue has been patched in version 0.9.6.	8.5	More Details
CVE-2025-44018	A firmware downgrade vulnerability exists in the OTA Update functionality of GL-Inet GL-AXT1800 4.7.0. A specially crafted .tar file can lead to a firmware downgrade. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.	8.3	More Details
CVE-2025-62459	Microsoft Defender Portal Spoofing Vulnerability	8.3	More Details
CVE-2025-13609	A vulnerability has been identified in keylime where an attacker can exploit this flaw by registering a new agent using a different Trusted Platform Module (TPM) device but claiming an existing agent's unique identifier (UUID). This action overwrites the legitimate agent's identity, enabling the attacker to impersonate the compromised agent and potentially bypass security controls.	8.2	More Details
CVE-2025-58360	GeoServer is an open source server that allows users to share and edit geospatial data. From version 2.26.0 to before 2.26.2 and before 2.25.6, an XML External Entity (XXE) vulnerability was identified. The application accepts XML input through a specific endpoint /geoserver/wms operation GetMap. However, this input is not sufficiently sanitized or restricted, allowing an attacker to define external entities within the XML request. This issue has been patched in GeoServer 2.25.6, GeoServer 2.26.3, and GeoServer 2.27.0.	8.2	More Details

CVE-2025-65025	esm.sh is a nobuild content delivery network(CDN) for modern web development. Prior to version 136, the esm.sh CDN service is vulnerable to path traversal during NPM package tarball extraction. An attacker can craft a malicious NPM package containing specially crafted file paths (e.g., package/../../tmp/evil.js). When esm.sh downloads and extracts this package, files may be written to arbitrary locations on the server, escaping the intended extraction directory. This issue has been patched in version 136.	8.2	More Details
CVE-2025-0248	HCL iNotes is susceptible to a Reflected Cross-site Scripting (XSS) vulnerability caused by improper validation of user-supplied input. A remote, unauthenticated attacker can specially craft a URL to execute script in a victim's Web browser within the security context of the hosting Web site and/or steal the victim's cookie-based authentication credentials.	8.1	More Details
CVE-2025-64759	Homarr is an open-source dashboard. Prior to version 1.43.3, stored XSS vulnerability exists, allowing the execution of arbitrary JavaScript in a user's browser, with minimal or no user interaction required, due to the rendering of a malicious uploaded SVG file. This could be abused to add an attacker's account to the "credentials-admin" group, giving them full administrative access, if a user logged in as an administrator was to view the page which renders or redirects to the SVG. This issue has been patched in version 1.43.3.	8.1	More Details
CVE-2025-65034	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an improper authorization vulnerability allows any authenticated user to reopen finalized polls belonging to other users by manipulating the pollId parameter. This can disrupt events managed by other users and compromise both availability and integrity of poll data. This issue has been patched in version 4.5.4.	8.1	More Details
CVE-2025-13316	Twonky Server 8.5.2 on Linux and Windows is vulnerable to a cryptographic flaw, use of hard-coded cryptographic keys. An attacker with knowledge of the encrypted administrator password can decrypt the value with static keys to view the plain text password and gain administrator-level access to Twonky Server.	8.1	More Details
CVE-2025-65029	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an insecure direct object reference (IDOR) vulnerability allows any authenticated user to delete arbitrary participants from polls without ownership verification. The endpoint relies solely on a participant ID to authorize deletions, enabling attackers to remove other users (including poll owners) from polls. This impacts the integrity and availability of poll participation data. This issue has been patched in version 4.5.4.	8.1	More Details
CVE-2025-65033	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an authorization flaw in the poll management feature allows any authenticated user to pause or resume any poll, regardless of ownership. The system only uses the public pollId to identify polls, and it does not verify whether the user performing the action is the poll owner. As a result, any user can disrupt polls created by others, leading to a loss of integrity and availability across the application. This issue has been patched in version 4.5.4.	8.1	More Details
CVE-2025-65946	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Prior to version 3.26.7, Due to an error in validation it was possible for Roo to automatically execute commands that did not match the allow list prefixes. This issue has been patched in version 3.26.7.	8.1	More Details
CVE-2025-60915	An issue in the size query parameter (/views/file.py) of Austrian Archaeological Institute Openatlas before v8.12.0 allows attackers to execute a path traversal via a crafted request.	8.1	More Details
CVE-2025-	The WP AUDIO GALLERY plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in all versions up to, and including, 2.0. This is due to the `wpag_uploadaudio_callback()` AJAX handler not properly validating user-supplied file paths in the `audio_upload` parameter before passing them to `unlink()`. This	8.1	More Details

13322	makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when critical files like wp-config.php are deleted.		
CVE-2025-64660	Improper access control in GitHub Copilot and Visual Studio Code allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2025-33188	NVIDIA DGX Spark GB10 contains a vulnerability in hardware resources where an attacker could tamper with hardware controls. A successful exploit of this vulnerability might lead to information disclosure, data tampering, or denial of service.	8.0	More Details
CVE-2025-52538	Improper input validation within the XOCL driver may allow a local attacker to generate an integer overflow condition, potentially resulting in loss of confidentiality or availability.	8.0	More Details
CVE-2025-13035	The Code Snippets plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 3.9.1. This is due to the plugin's use of extract() on attacker-controlled shortcode attributes within the `evaluate_shortcode_from_flat_file` method, which can be used to overwrite the `$filepath` variable and subsequently passed to require_once. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute arbitrary PHP code on the server via the `[code_snippet]` shortcode using PHP filter chains granted they can trick an administrator into enabling the "Enable file-based execution" setting and creating at least one active Content snippet.	8.0	More Details
CVE-2025-40890	A Stored Cross-Site Scripting vulnerability was discovered in the Dashboards functionality due to improper validation of an input parameter. An authenticated low-privilege user can craft a malicious dashboard containing a JavaScript payload and share it with victim users, or a victim can be socially engineered to import a malicious dashboard template. When the victim views or imports the dashboard, the XSS executes in their browser context, allowing the attacker to perform unauthorized actions as the victim, such as modify application data, disrupt application availability, and access limited sensitive information.	7.9	More Details
CVE-2025-13499	Kafka dissector crash in Wireshark 4.6.0 and 4.4.0 to 4.4.10 allows denial of service	7.8	More Details
CVE-2025-11001	7-Zip ZIP File Parsing Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of 7-Zip. Interaction with this product is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the handling of symbolic links in ZIP files. Crafted data in a ZIP file can cause the process to traverse to unintended directories. An attacker can leverage this vulnerability to execute code in the context of a service account. Was ZDI-CAN-26753.	7.8	More Details
CVE-2025-33204	NVIDIA NeMo Framework for all platforms contains a vulnerability in the NLP and LLM components, where malicious data created by an attacker could cause code injection. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-33189	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause an out-of-bound write. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, information disclosure, or escalation of privileges.	7.8	More Details
CVE-2025-30201	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to version 4.13.0, a vulnerability in Wazuh Agent allows authenticated attackers to force NTLM authentication through malicious UNC paths in various agent configuration settings, potentially leading NTLM relay attacks that would result	7.7	More Details

	privilege escalation and remote code execution. This issue has been patched in version 4.13.0.		
CVE-2025-56401	ZIRA Group WBRM 7.0 is vulnerable to SQL Injection in referenceLookupsByTableNameAndColumnName.	7.6	More Details
CVE-2025-33203	NVIDIA NeMo Agent Toolkit UI for Web contains a vulnerability in the chat API endpoint where an attacker may cause a Server-Side Request Forgery. A successful exploit of this vulnerability may lead to information disclosure and denial of service.	7.6	More Details
CVE-2025-54338	An Incorrect Access Control vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows an attacker to disclose user hashes.	7.5	More Details
CVE-2025-63889	The fetch function in file thinkphp\library\think\Template.php in ThinkPHP 5.0.24 allows attackers to read arbitrary files via crafted file path in a template value.	7.5	More Details
CVE-2025-7402	The Ads Pro Plugin - Multi-Purpose WordPress Advertising Manager plugin for WordPress is vulnerable to time-based SQL Injection via the ‘site_id’ parameter in all versions up to, and including, 4.95 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.	7.5	More Details
CVE-2025-41075	Vulnerability in LimeSurvey 6.13.0 in the endpoint /optin that causes infinite HTTP redirects when accessed directly. This behavior can be exploited to generate a Denegation of Service (DoS attack), by exhausting server or client resources. The system is unable to break the redirect loop, which can cause service degradation or browser instability.	7.5	More Details
CVE-2025-13526	The OneClick Chat to Order plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.0.8 via the 'wa_order_thank_you_override' function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to view sensitive customer information including names, email addresses, phone numbers, billing/shipping addresses, order contents, and payment methods by simply changing the order ID in the URL.	7.5	More Details
CVE-2025-13470	In RNP version 0.18.0 a refactoring regression causes the symmetric session key used for Public-Key Encrypted Session Key (PKESK) packets to be left uninitialized except for zeroing, resulting in it always being an all-zero byte array. Any data encrypted using public-key encryption in this release can be decrypted trivially by supplying an all-zero session key, fully compromising confidentiality. The vulnerability affects only public key encryption (PKESK packets). Passphrase-based encryption (SKESK packets) is not affected. Root cause: Vulnerable session key buffer used in PKESK packet generation. The defect was introduced in commit `7bd9a8dc356aae756b40755be76d36205b6b161a` where initialization logic inside `encrypted_build_skesk()` only randomized the key for the SKESK path and omitted it for the PKESK path.	7.5	More Details
CVE-2025-13502	A flaw was found in WebKitGTK and WPE WebKit. This vulnerability allows an out-of-bounds read and integer underflow, leading to a UIProcess crash (DoS) via a crafted payload to the GLib remote inspector server.	7.5	More Details
CVE-2025-63205	An issue was discovered in bridgetech probes VB220 IP Network Probe,VB120 Embedded IP + RF Probe, VB330 High-Capacity Probe, VB440 ST 2110 Production Analytics Probe, and NOMAD, firmware versions 6.5.0-9, allowing attackers to gain sensitive information such as administrator passwords via the /probe/core/setup/passwd endpoint.	7.5	More Details

CVE-2025-13384	The CP Contact Form with PayPal plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.3.56. This is due to the plugin exposing an unauthenticated IPN-like endpoint (via the 'cp_contactformpp_ipncheck' query parameter) that processes payment confirmations without any authentication, nonce verification, or PayPal IPN signature validation. This makes it possible for unauthenticated attackers to mark form submissions as paid without making actual payments by sending forged payment notification requests with arbitrary POST data (payment_status, txn_id, payer_email).	7.5	More Details
CVE-2025-63209	The ELCA Star Transmitter Remote Control firmware 1.25 for STAR150, BP1000, STAR300, STAR2000, STAR1000, STAR500, and possibly other models, contains an information disclosure vulnerability allowing unauthenticated attackers to retrieve admin credentials and system settings via an unprotected /setup.xml endpoint. The admin password is stored in plaintext under the <p05> XML tag, potentially leading to remote compromise of the transmitter system.	7.5	More Details
CVE-2025-63371	Milos Paripovic OneCommander 3.102.0.0 is vulnerable to Directory Traversal. The vulnerability resides in the ZIP file processing component, specifically in the functionality responsible for extracting and handling ZIP archive contents.	7.5	More Details
CVE-2025-51663	A vulnerability found in IPRateLimit implementation of FileCodeBox up to 2.2 allows remote attackers to bypass ip-based rate limit protection and failed attempt restrictions by faking X-Real-IP and X-Forwarded-For HTTP headers. This can enable attackers to perform DoS attacks or brute force share codes.	7.5	More Details
CVE-2025-63208	An issue was discovered in bridgetech VB288 Objective QoE Content Extractor, firmware version 5.6.0-8, allowing attackers to gain sensitive information such as administrator passwords via the /probe/core/setup/passwd endpoint.	7.5	More Details
CVE-2025-54563	An Incorrect Access Control vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows Incorrect Access Control, leading to Remote Information Disclosure.	7.5	More Details
CVE-2025-62294	SOPlanning is vulnerable to Predictable Generation of Password Recovery Token. Due to weak mechanism of generating recovery tokens, a malicious attacker is able to brute-force all possible values and takeover any account in reasonable amount of time. This issue was fixed in version 1.55.	7.5	More Details
CVE-2025-63700	An issue was discovered in Clerk-js 5.88.0 allowing attackers to bypass the OAuth authentication flow by manipulating the request at the OTP verification stage.	7.5	More Details
CVE-2025-41074	Vulnerability in LimeSurvey 6.13.0 in the endpoint /optout that causes infinite HTTP redirects when accessed directly. This behavior can be exploited to generate a Denegation of Service (DoS attack), by exhausting server or client resources. The system is unable to break the redirect loop, which can cause service degradation or browser instability.	7.5	More Details
CVE-2025-11230	Inefficient algorithm complexity in mjson in HAProxy allows remote attackers to cause a denial of service via specially crafted JSON requests.	7.5	More Details
CVE-2025-51741	An issue was discovered in Veal98 Echo Open-Source Community System 2.2 thru 2.3 allowing an unauthenticated attacker to cause the server to send email verification messages to arbitrary users via the /sendEmailCodeForResetPwd endpoint potentially causing a denial of service to the server or the downstream users.	7.5	More Details
CVE-2025-61138	Qlik Sense Enterprise v14.212.13 was discovered to contain an information leak via the /dev-hub/ directory.	7.5	More Details

CVE-2025-13138	The WP Directory Kit plugin for WordPress is vulnerable to SQL Injection via the 'columns_search' parameter of the select_2_ajax() function in all versions up to, and including, 1.4.3 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.	7.5	More Details
CVE-2025-63219	The ITEL ISO FM SFN Adapter (firmware ISO2 2.0.0.0, WebServer 2.0) is vulnerable to session hijacking due to improper session management on the /home.html endpoint. An attacker can access an active session without authentication, allowing them to control the device, modify configurations, and compromise system integrity.	7.5	More Details
CVE-2025-65503	Use after free in endpoint destructors in Redboltz async_mqtt 10.2.5 allows local users to cause a denial of service via triggering SSL initialization failure that results in incorrect destruction order between io_context and endpoint objects.	7.5	More Details
CVE-2025-65495	Integer signedness error in tls_verify_call_back() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted TLS certificate that causes i2d_X509() to return -1 and be misused as a malloc() size parameter.	7.5	More Details
CVE-2025-25613	FS Inc S3150-8T2F 8-Port Gigabit Ethernet L2+ Switch, 8 x Gigabit RJ45, with 2 x 1Gb SFP, Fanless. All versions before 2.2.0D Build 135103 were discovered to transmit cookies for their web based administrative application containing usernames and passwords. These were transmitted in cleartext using simple base64 encoding during every POST request made to the server.	7.5	More Details
CVE-2025-65494	NULL pointer dereference in get_san_or_cn_from_cert() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted X.509 certificate that causes sk_GENERAL_NAME_value() to return NULL.	7.5	More Details
CVE-2025-65493	NULL pointer dereference in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted DTLS/TLS connection that triggers BIO_get_data() to return NULL.	7.5	More Details
CVE-2025-40601	A Stack-based buffer overflow vulnerability in the SonicOS SSLVPN service allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash.	7.5	More Details
CVE-2025-51661	A path Traversal vulnerability found in FileCodeBox v2.2 and earlier allows arbitrary file writes when application is configured to use local filesystem storage. SystemFileStorage.save_file method in core/storage.py uses filenames from user input without validation to construct save_path and save files. This allows remote attackers to perform arbitrary file writes outside the intended directory by sending crafted POST requests with malicious traversal sequences to /share/file/ upload endpoint, which does not require any authorization.	7.5	More Details
CVE-2025-60638	An issue was discovered in Free5GC v4.0.0 and v4.0.1 allowing an attacker to cause a denial of service via crafted POST request to the Nnssf_NSSAIAvailability API.	7.5	More Details
CVE-2025-41729	An unauthenticated remote attacker can send a specially crafted Modbus read command to the device which leads to a denial of service.	7.5	More Details
CVE-2025-12646	The Community Events plugin for WordPress is vulnerable to SQL Injection via the 'dayofyear' parameter in all versions up to, and including, 1.5.4 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.	7.5	More Details
	Apache Syncope can be configured to store the user password values in the internal		

CVE-2025-65998	database with AES encryption, though this is not the default option. When AES is configured, the default key value, hard-coded in the source code, is always used. This allows a malicious attacker, once obtained access to the internal database content, to reconstruct the original cleartext password values. This is not affecting encrypted plain attributes, whose values are also stored using AES encryption. Users are recommended to upgrade to version 3.0.15 / 4.0.3, which fix this issue.	7.5	More Details
CVE-2025-13357	Vault's Terraform Provider incorrectly set the default deny_null_bind parameter for the LDAP auth method to false by default, potentially resulting in an insecure configuration. If the underlying LDAP server allowed anonymous or unauthenticated binds, this could result in authentication bypass. This vulnerability, CVE-2025-13357, is fixed in Vault Terraform Provider v5.5.0.	7.4	More Details
CVE-2025-13132	This vulnerability allowed a site to enter fullscreen, after a user click, without a full-screen notification (toast) appearing. Without this notification, users could potentially be misled about what site they were on if a malicious site renders a fake UI (like a fake address bar.)	7.4	More Details
CVE-2025-13410	A vulnerability has been found in Campcodes Retro Basketball Shoes Online Store 1.0. Affected is an unknown function of the file /admin/receipt.php. Such manipulation of the argument tid leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-13572	A vulnerability was identified in projectworlds Advanced Library Management System 1.0. This affects an unknown part of the file /delete_admin.php. The manipulation of the argument admin_id leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-13562	A vulnerability was identified in D-Link DIR-852 1.00. This issue affects some unknown processing of the file /gena.cgi. Such manipulation of the argument service leads to command injection. The attack can be executed remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2025-63719	Campcodes Online Hospital Management System 1.0 is vulnerable to SQL Injection in /admin/index.php via the parameter username.	7.3	More Details
CVE-2025-13420	A weakness has been identified in itsourcecode Human Resource Management System 1.0. This issue affects some unknown processing of the file /src/store/EventStore.php. This manipulation of the argument eventSubject causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-13421	A security vulnerability has been detected in itsourcecode Human Resource Management System 1.0. Impacted is an unknown function of the file /src/store/NoticeStore.php. Such manipulation of the argument noticeDesc leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13422	A vulnerability was detected in freeprojectscodes Sports Club Management System 1.0. The affected element is an unknown function of the file /dashboard/admin/change_s_pwd.php. Performing manipulation of the argument login_id results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-13561	A vulnerability was determined in SourceCodester Company Website CMS 1.0. This vulnerability affects unknown code of the file /admin/index.php. This manipulation of the argument Username causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details

CVE-2025-13557	A vulnerability has been found in Campcodes Online Polling System 1.0. Affected by this issue is some unknown functionality of the file /registeracc.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.	7.3	More Details
CVE-2024-21923	Incorrect default permissions in AMD StoreMI™ could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2024-21922	A DLL hijacking vulnerability in AMD StoreMI™ could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2025-13556	A flaw has been found in Campcodes Online Polling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/checklogin.php. Executing manipulation of the argument myusername can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-13442	A security vulnerability has been detected in UTT 进取 750W up to 3.2.2-191225. Affected by this vulnerability is the function system of the file /goform/formPdbUpConfig. Such manipulation of the argument policyNames leads to command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-13555	A vulnerability was detected in Campcodes School File Management System 1.0. Affected is an unknown function of the file /index.php of the component Login. Performing manipulation of the argument stud_no results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-13449	A vulnerability was found in code-projects Online Shop Project 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument Password results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-13560	A vulnerability was found in SourceCodester Company Website CMS 1.0. This affects an unknown part of the file /admin/reset-password.php. The manipulation of the argument email results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-13585	A vulnerability was detected in code-projects COVID Tracking System 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument code results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2025-63932	D-Link Router DIR-868L A1 FW106KRb01.bin has an unauthenticated remote code execution vulnerability in the cgibin binary. The HNAP service provided by cgibin does not filter the HTTP SOAPAction header field. The unauthenticated remote attacker can execute the shell command.	7.3	More Details
CVE-2025-13583	A weakness has been identified in code-projects Question Paper Generator 1.0. This affects an unknown part of the file /signupscript.php of the component POST Parameter Handler. Executing manipulation of the argument Fname can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-0003	Inadequate lock protection within Xilinx Run time may allow a local attacker to trigger a Use-After-Free condition potentially resulting in loss of confidentiality or availability	7.3	More Details
CVE-2025-	A buffer overflow with Xilinx Run Time Environment may allow a local attacker to read or corrupt data from the advanced extensible interface (AXI), potentially resulting in	7.3	More

52539	loss of confidentiality, integrity, and/or availability.		Details
CVE-2025-0005	Improper input validation within the XOCL driver may allow a local attacker to generate an integer overflow condition, potentially resulting in crash or denial of service.	7.3	More Details
CVE-2025-13485	A security flaw has been discovered in itsourcecode Online File Management System 1.0. This issue affects some unknown processing of the file /ajax.php?action=login. The manipulation of the argument Username results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-13395	A security flaw has been discovered in codehub666 94list up to 5831c8240e99a72b7d3508c79ef46ae4b96befe8. The impacted element is the function Login of the file /function.php. The manipulation results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	7.3	More Details
CVE-2025-66079	Missing Authorization vulnerability in Jegstudio Gutenverse Form gutenverse-form allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gutenverse Form: from n/a through <= 2.2.0.	7.3	More Details
CVE-2025-13451	A vulnerability was identified in SourceCodester Online Shop Project 1.0. The affected element is an unknown function of the file /action.php. Such manipulation of the argument Search leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-13554	A security vulnerability has been detected in Campcodes Supplier Management System 1.0. This impacts an unknown function of the file /index.php of the component Login. Such manipulation of the argument txtUsername leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13582	A security flaw has been discovered in code-projects Jonnys Liquor 1.0. Affected by this issue is some unknown functionality of the file /detail.php of the component GET Parameter Handler. Performing manipulation of the argument Product results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-13578	A vulnerability has been found in code-projects Library System 1.0. This affects an unknown function of the file /index.php of the component Login. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-12120	Lite XL versions 2.1.8 and prior automatically execute the .lite_project.lua file when opening a project directory, without prompting the user for confirmation. The .lite_project.lua file is intended for project-specific configuration but can contain executable Lua logic. This behavior could allow execution of untrusted Lua code if a user opens a malicious project, potentially leading to arbitrary code execution with the privileges of the Lite XL process.	7.3	More Details
CVE-2025-12121	Lite XL versions 2.1.8 and prior contain a vulnerability in the system.exec function, which allowed arbitrary command execution through unsanitized shell command construction. This function was used in project directory launching (core.lua), drag-and-drop file handling (rootview.lua), and the “open in system” command in the treeview plugin (treeview.lua). If an attacker could influence input to system.exec, they might execute arbitrary commands with the privileges of the Lite XL process.	7.3	More Details
CVE-2025-33205	NVIDIA NeMo framework contains a vulnerability in a predefined variable, where an attacker could cause inclusion of functionality from an untrusted control sphere by use of a predefined variable. A successful exploit of this vulnerability may lead to code execution.	7.3	More Details

CVE-2025-13376	The ProjectList plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in all versions up to, and including, 0.3.0. This makes it possible for authenticated attackers, with Editor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-12135	The WPBookit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'css_code' parameter in all versions up to, and including, 1.0.6 due to a missing capability check on the save_custome_code() function. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-12160	The Simple User Registration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpr_admin_msg' parameter in all versions up to, and including, 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 will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-13145	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 7.33.1. This is due to deserialization of untrusted data supplied via CSV file imports in the import_single_post_as_csv function within SingleImportExport.php. This makes it possible for authenticated attackers, with administrator-level access or higher, to inject a PHP object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	7.2	More Details
CVE-2025-12484	The Giveaways and Contests by RafflePress – Get More Website Traffic, Email Subscribers, and Social Followers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple social media username parameters in all versions up to, and including, 1.12.19 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.	7.2	More Details
CVE-2025-13206	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘name’ parameter in all versions up to, and including, 4.13.0 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. Avatars must be enabled in the WordPress install in order to exploit the vulnerability.	7.2	More Details
CVE-2025-12973	The S2B AI Assistant – ChatBot, ChatGPT, OpenAI, Content & Image Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the storeFile() function in all versions up to, and including, 1.7.8. This makes it possible for authenticated attackers, with Editor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-63220	The Sound4 FIRST web-based management interface is vulnerable to Remote Code Execution (RCE) via a malicious firmware update package. The update mechanism fails to validate the integrity of manual.sh, allowing an attacker to inject arbitrary commands by modifying this script and repackaging the firmware.	7.2	More Details
CVE-2025-0645	Unrestricted Upload of File with Dangerous Type vulnerability in Narkom Communication and Software Technologies Trade Ltd. Co. Pyxis Signage allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Pyxis Signage: through 31012025.	7.2	More Details
CVE-2025-0643	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Narkom Communication and Software Technologies Trade Ltd. Co. Pyxis Signage allows Stored XSS.This issue affects Pyxis Signage: through	7.2	More Details

	31012025.		
CVE-2025-13068	The Telegram Bot & Channel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Telegram username in all versions up to, and including, 4.1 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.	7.2	More Details
CVE-2025-65022	i-Educar is free, fully online school management software. In versions 2.10.0 and prior, an authenticated time-based SQL injection vulnerability exists in the ieducar/intranet/agenda.php script. An attacker with access to an authenticated session can execute arbitrary SQL commands against the application's database. This vulnerability is caused by the improper handling of the cod_agenda request parameter, which is directly concatenated into multiple SQL queries without proper sanitization. This issue has been patched in commit b473f92.	7.2	More Details
CVE-2025-65023	i-Educar is free, fully online school management software. In versions 2.10.0 and prior, an authenticated time-based SQL injection vulnerability exists in the ieducar/intranet/funcionario_vinculo_cad.php script. An attacker with access to an authenticated session can execute arbitrary SQL commands against the application's database. This vulnerability is caused by the improper handling of the cod_funcionario_vinculo GET parameter, which is directly concatenated into an SQL query without proper sanitization. This issue has been patched in commit a00dfa3.	7.2	More Details
CVE-2025-65024	i-Educar is free, fully online school management software. In versions 2.10.0 and prior, an authenticated time-based SQL injection vulnerability exists in the ieducar/intranet/agenda_admin_cad.php script. An attacker with access to an authenticated session can execute arbitrary SQL commands against the application's database. This vulnerability is caused by the improper handling of the cod_agenda GET parameter, which is directly concatenated into an SQL query without proper sanitization. This issue has been patched in commit 3e9763a.	7.2	More Details
CVE-2025-64050	A Remote Code Execution (RCE) vulnerability in the template management component in REDAXO CMS 5.20.0 allows remote authenticated administrators to execute arbitrary operating system commands by injecting PHP code into an active template. The payload is executed when visitors access frontend pages using the compromised template.	7.2	More Details
CVE-2025-66055	Deserialization of Untrusted Data vulnerability in Icegram Email Subscribers & Newsletters email-subscribers allows Object Injection.This issue affects Email Subscribers & Newsletters: from n/a through <= 5.9.10.	7.2	More Details
CVE-2025-13159	The Flo Forms – Easy Drag & Drop Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file uploads in all versions up to, and including, 1.0.43. This is due to the plugin allowing SVG file uploads via an unauthenticated AJAX endpoint (`flo_form_submit`) without proper file content validation. This makes it possible for unauthenticated attackers to upload malicious SVG files containing JavaScript that executes when an administrator views the uploaded file in the WordPress admin interface, leading to potential full site compromise.	7.1	More Details
CVE-2025-48510	Improper return value within AMD uProf can allow a local attacker to bypass KSLR, potentially resulting in loss of confidentiality or availability.	7.1	More Details
CVE-2025-65018	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From version 1.6.0 to before 1.6.51, there is a heap buffer overflow vulnerability in the libpng simplified API function png_image_finish_read when processing 16-bit interlaced PNGs with 8-bit output format. Attacker-crafted interlaced PNG files cause heap writes beyond allocated buffer bounds. This issue has been patched in version 1.6.51.	7.1	More Details

CVE-2025-65030	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an authorization flaw in the comment deletion API allows any authenticated user to delete comments belonging to other users, including poll owners and administrators. The endpoint relies solely on the comment ID for deletion and does not validate whether the requesting user owns the comment or has permission to remove it. This issue has been patched in version 4.5.4.	7.1	More Details
CVE-2025-64720	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From version 1.6.0 to before 1.6.51, an out-of-bounds read vulnerability exists in png_image_read_composite when processing palette images with PNG_FLAG_OPTIMIZE_ALPHA enabled. The palette compositing code in png_init_read_transformations incorrectly applies background compositing during premultiplication, violating the invariant component ≤ alpha × 257 required by the simplified PNG API. This issue has been patched in version 1.6.51.	7.1	More Details
CVE-2025-12629	The Broken Link Manager WordPress plugin through 0.6.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	7.1	More Details
CVE-2024-14015	The WordPress eCommerce Plugin WordPress plugin through 2.9.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	7.1	More Details
CVE-2025-64764	Astro is a web framework. Prior to version 5.15.8, a reflected XSS vulnerability is present when the server islands feature is used in the targeted application, regardless of what was intended by the component template(s). This issue has been patched in version 5.15.8.	7.1	More Details
CVE-2025-13433	A security flaw has been discovered in Muse Group MuseHub 2.1.0.1567. The affected element is an unknown function of the file C:\Program Files\WindowsApps\Muse.MuseHub_2.1.0.1567_x64__rb9pth70m6nz6\Muse.Updater.exe of the component Windows Service. The manipulation results in unquoted search path. The attack is only possible with local access. A high complexity level is associated with this attack. The exploitability is described as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2025-62709	ClipBucket v5 is an open source video sharing platform. In ClipBucket version 5.5.2, a change to network.class.php causes the application to dynamically build the server URL from the incoming HTTP Host header when the configuration base_url is not set. Because Host is a client-controlled header, an attacker can supply an arbitrary Host value. This allows an attacker to cause password-reset links (sent by forget.php) to be generated with the attacker’s domain. If a victim follows that link and enters their activation code on the attacker-controlled domain, the attacker can capture the code and use it to reset the victim’s password and take over the account. This issue has been patched in version 5.5.2#162.	6.8	More Details
CVE-2025-64770	The affected products allow unauthenticated access to Open Network Video Interface Forum (ONVIF) services, which may allow an attacker unauthorized access to camera configuration information.	6.8	More Details
CVE-2025-65089	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Prior to version 1.27.0, a user with no view rights on a page may see the content of an office attachment displayed with the view file macro. This issue has been patched in version 1.27.0.	6.8	More Details
CVE-2025-62346	A Cross-Site Request Forgery (CSRF) vulnerability was identified in HCL Glovius Cloud. An attacker can force a user's web browser to execute an unwanted, malicious action on a trusted site where the user is authenticated, specifically on one endpoint.	6.8	More Details
CVE-2025-	The affected product allows unauthenticated access to Real Time Streaming Protocol (RTSP) services, which may allow an attacker unauthorized access to camera	6.8	More Details

62674	configuration information.		
CVE-2025-12502	The attention-bar WordPress plugin through 0.7.2.1 does not sanitize and escape a parameter before using it in a SQL statement, allowing high privilege users such as administrator to perform SQL injection attacks	6.8	More Details
CVE-2025-33190	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware where an attacker could cause an out-of-bound write. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, or escalation of privileges.	6.7	More Details
CVE-2025-65960	Contao is an Open Source CMS. From version 4.0.0 to before 4.13.57, before 5.3.42, and before 5.6.5, back end users with precise control over the contents of template closures can execute arbitrary PHP functions that do not have required parameters. This issue has been patched in versions 4.13.57, 5.3.42, and 5.6.5. A workaround for this issue involves manually patching the Contao\Template::once() method.	6.6	More Details
CVE-2025-66053	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kriesi Enfold enfold allows Stored XSS.This issue affects Enfold: from n/a through <= 7.1.2.	6.5	More Details
CVE-2025-61167	SIGB PMB v8.0.1.14 was discovered to contain multiple SQL injection vulnerabilities in the /opac_css/ajax_selector.php component via the id and datas parameters.	6.5	More Details
CVE-2025-65020	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an Insecure Direct Object Reference (IDOR) vulnerability in the poll duplication endpoint (/api/trpc/polls.duplicate) allows any authenticated user to duplicate polls they do not own by modifying the pollId parameter. This effectively bypasses access control and lets unauthorized users clone private or administrative polls. This issue has been patched in version 4.5.4.	6.5	More Details
CVE-2025-63953	A Cross-Site Request Forgery (CSRF) in the /usapi?method=add-user component of Magewell Pro Convert v1.2.213 allows attackers to arbitrarily create accounts via a crafted GET request.	6.5	More Details
CVE-2025-10144	The Perfect Brands for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the `brands` attribute of the `products` shortcode in all versions up to, and including, 3.6.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-12174	The Directorist: AI-Powered Business Directory Plugin with Classified Ads Listings plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the 'directorist_prepare_listings_export_file' and 'directorist_type_slug_change' AJAX actions in all versions up to, and including, 8.5.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export listing details and change the directorist slug.	6.5	More Details
CVE-2025-13380	The AI Engine for WordPress: ChatGPT, GPT Content Generator plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 1.0.1. This is due to insufficient validation of user-supplied file paths in the 'lqdai_update_post' AJAX endpoint and the use of file_get_contents() with user-controlled URLs without protocol restrictions in the insert_image() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-40604	Download of Code Without Integrity Check Vulnerability in the SonicWall Email Security appliance loads root filesystem images without verifying signatures, allowing attackers with VMDK or datastore access to modify system files and gain persistent arbitrary code execution.	6.5	More Details

CVE-2025-66098	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Camille V Travelers' Map travelers-map allows Stored XSS.This issue affects Travelers' Map: from n/a through <= 2.3.2.	6.5	More Details
CVE-2025-60632	An issue was discovered in Free5GC v4.0.0 and v4.0.1 allowing an attacker to cause a denial of service via crafted POST request to the Npcf_BDTPolicyControl API.	6.5	More Details
CVE-2025-66091	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Design Stylish Cost Calculator stylish-cost-calculator allows DOM-Based XSS.This issue affects Stylish Cost Calculator: from n/a through <= 8.1.5.	6.5	More Details
CVE-2025-66090	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Skill Bar skt-skill-bar allows DOM-Based XSS.This issue affects SKT Skill Bar: from n/a through <= 2.5.	6.5	More Details
CVE-2025-63914	An issue was discovered in Cinnamon kotaemon 0.11.0. The _may_extract_zip function in the \libs\ktem\ktem\index\file\ui.py file does not check the contents of uploaded ZIP files. Although the contents are extracted into a temporary folder that is cleared before each extraction, successfully uploading a ZIP bomb could still cause the server to consume excessive resources during decompression. Moreover, if no further files are uploaded afterward, the extracted data could occupy disk space and potentially render the system unavailable. Anyone with permission to upload files can carry out this attack.	6.5	More Details
CVE-2025-66073	Deserialization of Untrusted Data vulnerability in Cozmoslabs WP Webhooks wp-webhooks allows Object Injection.This issue affects WP Webhooks: from n/a through <= 3.3.8.	6.5	More Details
CVE-2025-62426	vLLM is an inference and serving engine for large language models (LLMs). From version 0.5.5 to before 0.11.1, the /v1/chat/completions and /tokenize endpoints allow a chat_template_kwargs request parameter that is used in the code before it is properly validated against the chat template. With the right chat_template_kwargs parameters, it is possible to block processing of the API server for long periods of time, delaying all other requests. This issue has been patched in version 0.11.1.	6.5	More Details
CVE-2025-63878	Github Restaurant Website Restoran v1.0 was discovered to contain a SQL injection vulnerability via the Contact Form page.	6.5	More Details
CVE-2025-60633	An issue was discovered in Free5GC v4.0.0 and v4.0.1 allowing an attacker to cause a denial of service via the Nudm_SubscriberDataManagement API.	6.5	More Details
CVE-2025-65028	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an insecure direct object reference (IDOR) vulnerability allows any authenticated user to modify other participants' votes in polls without authorization. The backend relies solely on the participantId parameter to identify which votes to update, without verifying ownership or poll permissions. This allows an attacker to alter poll results in their favor, directly compromising data integrity. This issue has been patched in version 4.5.4.	6.5	More Details
CVE-2025-41076	In version 6.13.0 of LimeSurvey, any external user can cause a 500 error in the survey system by sending a malformed session cookie. Instead of displaying a generic error message, the system exposes internal backend information, including the use of the Yii framework, the MySQL/MariaDB database engine, the table name 'lime_sessions', primary keys, and fragments of the content that caused the conflict. This information can simplify the collection of data about the internal architecture of the application by an attacker.	6.5	More Details
	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an		

CVE-2025-65031	improper authorization flaw in the comment creation endpoint allows authenticated users to impersonate any other user by altering the authorName field in the API request. This enables attackers to post comments under arbitrary usernames, including privileged ones such as administrators, potentially misleading other users and enabling phishing or social engineering attacks. This issue has been patched in version 4.5.4.	6.5	More Details
CVE-2025-13644	MongoDB Server may experience an invariant failure during batched delete operations when handling documents. The issue arises when the server mistakenly assumes the presence of multiple documents in a batch based solely on document size exceeding BSONObjMaxSize. This issue affects MongoDB Server v7.0 versions prior to 7.0.26, MongoDB Server v8.0 versions prior to 8.0.13, and MongoDB Server v8.1 versions prior to 8.1.2	6.5	More Details
CVE-2025-60794	Session tokens and passwords in couch-auth 0.21.2 are stored in JavaScript objects and remain in memory without explicit clearing in src/user.ts lines 700-707. This creates a window of opportunity for sensitive data extraction through memory dumps, debugging tools, or other memory access techniques, potentially leading to session hijacking.	6.5	More Details
CVE-2025-60797	phpPgAdmin 7.13.0 and earlier contains a SQL injection vulnerability in dataexport.php at line 118. The application directly executes user-supplied SQL queries from the $_REQUEST['query'] parameter without any sanitization or parameterization via $data->conn->Execute($_REQUEST['query']). An authenticated attacker can exploit this vulnerability to execute arbitrary SQL commands, potentially leading to complete database compromise, data theft, or privilege escalation.	6.5	More Details
CVE-2025-60798	phpPgAdmin 7.13.0 and earlier contains a SQL injection vulnerability in display.php at line 396. The application passes user-controlled input from $_REQUEST['query'] directly to the browseQuery function without proper sanitization. An authenticated attacker can exploit this vulnerability to execute arbitrary SQL commands through malicious query manipulation, potentially leading to complete database compromise.	6.5	More Details
CVE-2025-63214	An issue was discovered in bridgetech VBC Server & Element Manager, firmware version 6.5.0-10 , 6.5.0-9, allowing unauthorized attackers to delete and create arbitrary accounts.	6.5	More Details
CVE-2025-63212	GatesAir Flexiva-LX devices on firmware 1.0.13 and 2.0, including models LX100, LX300, LX600, and LX1000, expose sensitive session identifiers (sid) in the publicly accessible log file located at /log/Flexiva%20LX.log. An unauthenticated attacker can retrieve valid session IDs and hijack sessions without providing any credentials. This attack requires the legitimate user (admin) to have previously closed the browser window without logging out.	6.5	More Details
CVE-2025-36371	IBM i 7.2, 7.3, 7.4, 7.5, and 7.6 are impacted by obtaining an information vulnerability in the database plan cache implementation. A user with access to the database plan cache could see information they do not have authority to view.	6.5	More Details
CVE-2025-13507	Inconsistent object size validation in time series processing logic may result in later processing of oversized BSON documents leading to an assert failing and process termination. This issue impacts MongoDB Server v7.0 versions prior to 7.0.26, v8.0 versions prior to 8.0.16 and MongoDB server v8.2 versions prior to 8.2.1.	6.5	More Details
CVE-2025-65107	Langfuse is an open source large language model engineering platform. In versions from 2.95.0 to before 2.95.12 and from 3.17.0 to before 3.131.0, in SSO provider configurations without an explicit AUTH_<PROVIDER>_CHECK setting, a potential account takeover may happen if an authenticated user is made to call a specifically crafted URL via a CSRF or phishing attack. This issue has been patched in versions 2.95.12 and 3.131.0. A workaround for this issue involves setting AUTH_<PROVIDER>_CHECK.	6.5	More Details
	Fluent Bit in_forward input plugin does not properly enforce the security.users authentication mechanism under certain configuration conditions. This allows remote		

CVE-2025-12969	attackers with network access to the Fluent Bit instance exposing the forward input to send unauthenticated data. By bypassing authentication controls, attackers can inject forged log records, flood alerting systems, or manipulate routing decisions, compromising the authenticity and integrity of ingested logs.	6.5	More Details
CVE-2025-65032	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an Insecure Direct Object Reference (IDOR) vulnerability allows any authenticated user to change the display names of other participants in polls without being an admin or the poll owner. By manipulating the participantId parameter in a rename request, an attacker can modify another user's name, violating data integrity and potentially causing confusion or impersonation attacks. This issue has been patched in version 4.5.4.	6.5	More Details
CVE-2025-10938	The UiPress lite plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.5.08. This is due to missing capability checks in the 'uip_process_block_query' AJAX function. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract sensitive user data including password hashes, emails, and other user information that could be used for account takeover attacks.	6.5	More Details
CVE-2025-12040	The Wishlist for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.0.9 via several functions in class-th-wishlist-frontend.php due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to modify other user's wishlists	6.5	More Details
CVE-2025-11003	The UiPress lite | Effortless custom dashboards, admin themes and pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'uip_save_ui_template' function in all versions up to, and including, 3.5.08. This makes it possible for authenticated attackers, with Subscriber-level access and above, to save templates that contain custom JavaScript.	6.4	More Details
CVE-2025-11767	The Tips Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tip' shortcode in all versions up to, and including, 0.2.1. This is 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.	6.4	More Details
CVE-2025-11799	The Affiliate AI Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'asin' shortcode attribute in the affiai_img shortcode in all versions up to, and including, 1.0.1. This is 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.	6.4	More Details
CVE-2025-13054	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wppb-embed shortcode in all versions up to, and including, 3.14.8 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.	6.4	More Details
CVE-2025-12661	The Pollcaster Shortcode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'height' parameter in the 'pollcaster' shortcode in all versions up to, and including, 1.0. This is 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.	6.4	More Details
	The FunnelKit – Funnel Builder for WooCommerce Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `wfop_phone` shortcode in all versions		

CVE-2025-12878	up to, and including, 3.13.1.2. This is due to insufficient input sanitization and output escaping on the user-supplied `default` attribute. 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.	6.4	More Details
CVE-2025-12964	The Magical Products Display plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mpdpr_title_tag' and 'mpdpr_subtitle_tag' parameters in the MPD Pricing Table widget in all versions up to, and including, 1.1.29 due to insufficient input sanitization and output escaping on user-supplied HTML tag names. 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.	6.4	More Details
CVE-2025-11802	The Bulma Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' shortcode attribute in the bulma-notification shortcode in all versions up to, and including, 1.0. This is 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.	6.4	More Details
CVE-2025-11770	The BrightTALK WordPress Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'format' shortcode attribute in the brighttalk-time shortcode in all versions up to, and including, 2.4.0. This is 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.	6.4	More Details
CVE-2025-11768	The Islamic Phrases plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'phrases' shortcode attribute in all versions up to, and including, 2.12.2015. This is 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.	6.4	More Details
CVE-2025-12710	The Pet-Manager – Petfinder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the kwm-petfinder shortcode in all versions up to, and including, 3.6.1 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.	6.4	More Details
CVE-2025-11803	The WPSite Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'format' shortcode attribute in the wpsite_y shortcode and the 'before' attribute in the wpsite_postauthor shortcode in all versions up to, and including, 1.2. This is due to insufficient input sanitization and output escaping in error messages. 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.	6.4	More Details
CVE-2025-13141	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Gutenberg blocks in all versions up to, and including, 3.0.0 due to insufficient input validation on user-supplied HTML tag names. This is due to the lack of a tag name whitelist allowing dangerous tags like 'script', 'iframe', and 'object' to be injected even though tag_escape() is used for sanitization. While some blocks use esc_html() for content, this can be bypassed using JavaScript encoding techniques (unquoted strings, backticks, String.fromCharCode()). 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.	6.4	More Details
	The Stock Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the		

CVE-2025-11765	'image_height' and 'image_width' shortcode attributes in all versions up to, and including, 1.1. This is 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.	6.4	More Details
CVE-2025-6251	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via $item['field_id'] in all versions up to, and including, 1.7.1036 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.	6.4	More Details
CVE-2025-13135	The HotelRunner Booking Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'hotelrunner' shortcode in all versions up to, and including, 5.2.4 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.	6.4	More Details
CVE-2025-11826	The WP Company Info plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' attribute of the 'social-networks' shortcode in all versions up to, and including, 1.9.0 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.	6.4	More Details
CVE-2025-12660	The Padlet Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'key' parameter in the 'wallwisher' shortcode in all versions up to, and including, 1.3. This is 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.	6.4	More Details
CVE-2025-11763	The Display Pages Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'column_count' parameter in the [display-pages] shortcode in all versions up to, and including, 1.1. This is 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.	6.4	More Details
CVE-2025-11808	The Shortcode for Google Street View plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'streetview' shortcode in all versions up to, and including, 0.5.7. This is due to insufficient input sanitization and output escaping on the 'id' attribute. 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.	6.4	More Details
CVE-2025-11764	The Shortcodes Bootstrap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' parameter in the [notification] shortcode in all versions up to, and including, 1.1. This is due to missing 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.	6.4	More Details
CVE-2025-11801	The AudioTube plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'caption' shortcode attribute of the 'audiotube' shortcode in all versions up to, and including, 0.0.3. This is 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.	6.4	More Details

CVE-2025-11800	The Surbma | MiniCRM Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute of the 'minicrm' shortcode in all versions up to, and including, 2.0. This is 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.	6.4	More Details
CVE-2025-12645	The Inline frame – Iframe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embedsite' shortcode in all versions up to, and including, 0.1. This is 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.	6.4	More Details
CVE-2025-12935	The FluentCRM – Email Newsletter, Automation, Email Marketing, Email Campaigns, Optins, Leads, and CRM Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'fluentcrm_content' shortcode in all versions up to, and including, 2.9.84 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.	6.4	More Details
CVE-2025-5092	Multiple plugins and/or themes for WordPress are vulnerable to Stored Cross-Site Scripting via the plugin's bundled lightGallery library (<= 2.8.3) in various versions 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.	6.4	More Details
CVE-2025-12800	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.4.5 via the su_shortcode_csv_table function. This makes it possible for authenticated attackers, with Administrator-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. If the 'Unsafe features' option is explicitly enabled by an administrator, this issue becomes exploitable by Contributor+ attackers	6.4	More Details
CVE-2025-11186	The Cookie Notice & Compliance for GDPR / CCPA plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cookies_accepted shortcode in all versions up to, and including, 2.5.8 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.	6.4	More Details
CVE-2025-13576	A vulnerability was detected in code-projects Blog Site 1.0. The affected element is an unknown function of the file /admin.php. Performing manipulation results in improper authorization. It is possible to initiate the attack remotely. The exploit is now public and may be used. Multiple endpoints are affected.	6.3	More Details
CVE-2025-36149	IBM Concert Software 1.0.0 through 2.0.0 could allow a remote attacker to hijack the clicking action of the victim.	6.3	More Details
CVE-2025-13544	A weakness has been identified in ashraf-kabir travel-agency up to 1f25aa03544bc5fb7a9e846f8a7879cecdb0cad3. Affected is an unknown function of the file /customer_register.php. Executing manipulation can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did	6.3	More Details

	not respond in any way.		
CVE-2025-13546	A vulnerability was detected in ashraf-kabir travel-agency up to 1f25aa03544bc5fb7a9e846f8a7879cecdb0cad3. Affected by this issue is some unknown functionality of the file /results.php of the component Search. The manipulation of the argument user_query results in sql injection. The attack can be launched remotely. The exploit is now public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	6.3	More Details
CVE-2025-13569	A vulnerability has been found in itsourcecode COVID Tracking System 1.0. Affected is an unknown function of the file /admin/?page=city. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-13579	A vulnerability was found in code-projects Library System 1.0. This impacts an unknown function of the file /return.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-13580	A vulnerability was determined in code-projects Library System 1.0. Affected is an unknown function of the file /mail.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-13573	A security flaw has been discovered in projectworlds can pass malicious payloads up to 1.0. This vulnerability affects unknown code of the file /add_book.php. The manipulation of the argument image results in unrestricted upload. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-64408	Apache Causeway faces Java deserialization vulnerabilities that allow remote code execution (RCE) through user-controllable URL parameters. These vulnerabilities affect all applications using Causeway's ViewModel functionality and can be exploited by authenticated attackers to execute arbitrary code with application privileges. This issue affects all current versions. Users are recommended to upgrade to version 3.5.0, which fixes the issue.	6.3	More Details
CVE-2025-13581	A vulnerability was identified in itsourcecode Student Information System 1.0. Affected by this vulnerability is an unknown functionality of the file /schedule_edit1.php. Such manipulation of the argument schedule_id leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-13567	A vulnerability was detected in itsourcecode COVID Tracking System 1.0. This affects an unknown function of the file /admin/?page=establishment. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-13568	A flaw has been found in itsourcecode COVID Tracking System 1.0. This impacts an unknown function of the file /admin/?page=people. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-13588	A vulnerability was found in lKinderBueno Streamity Xtream IPTV Player up to 2.8. The impacted element is an unknown function of the file public/proxy.php. Performing manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit has been made public and could be used. Upgrading to version 2.8.1 is sufficient to resolve this issue. The patch is named c70bfb8d36b47bfd64c5ec73917e1d9ddb97af92. It is suggested to upgrade the affected component.	6.3	More Details
CVE-	The WP 2FA WordPress plugin does not generate backup codes with enough entropy,		More

2025-12628	which could allow attackers to bypass the second factor by brute forcing them	6.3	Details
CVE-2025-66057	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in boldthemes Bold Page Builder bold-page-builder allows DOM-Based XSS.This issue affects Bold Page Builder: from n/a through <= 5.5.2.	6.3	More Details
CVE-2025-13571	A vulnerability was determined in code-projects Simple Food Ordering System 1.0. Affected by this issue is some unknown functionality of the file /listorder.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-13396	A weakness has been identified in code-projects Courier Management System 1.0. This affects an unknown function of the file /add-office.php. This manipulation of the argument OfficeName causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-13570	A vulnerability was found in itsourcecode COVID Tracking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/?page=state. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-13575	A security vulnerability has been detected in code-projects Blog Site 1.0. Impacted is the function category_exists of the file /resources/functions/blog.php of the component Category Handler. Such manipulation of the argument name/field leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. Multiple endpoints are affected.	6.3	More Details
CVE-2025-13087	A vulnerability exists in the Opto22 Groov Manage REST API on GRV-EPIC and groov RIO Products that allows remote code execution with root privileges. When a POST request is executed against the vulnerable endpoint, the application reads certain header details and unsafely uses these values to build commands, allowing an attacker with administrative privileges to inject arbitrary commands that execute as root.	6.2	More Details
CVE-2025-36159	IBM Concert 1.0.0 through 2.0.0 could allow a local user to forge log files to impersonate other users or hide their identity due to improper neutralization of output.	6.2	More Details
CVE-2025-63498	alinto SOGo 5.12.3 is vulnerable to Cross Site Scripting (XSS) via the "userName" parameter.	6.1	More Details
CVE-2025-64505	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. Prior to version 1.6.51, a heap buffer over-read vulnerability exists in libpng's png_do_quantize function when processing PNG files with malformed palette indices. The vulnerability occurs when palette_lookup array bounds are not validated against externally-supplied image data, allowing an attacker to craft a PNG file with out-of-range palette indices that trigger out-of-bounds memory access. This issue has been patched in version 1.6.51.	6.1	More Details
CVE-2025-64048	YCCMS 3.4 contains a stored cross-site scripting (XSS) vulnerability in the article management functionality. The vulnerability exists in the add() and getPost() functions within the ArticleAction.class.php file due to improper neutralization of user input in the article title field.	6.1	More Details
CVE-2025-64047	OpenRapid RapidCMS 1.3.1 is vulnerable to Cross Site Scripting (XSS) in /user/user-move.php.	6.1	More Details
CVE-	The Tainacan plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search' parameter in all versions up to, and including, 1.0.0 due to insufficient		More

2025-12746	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.	6.1	Details
CVE-2025-13383	The Job Board by BestWebSoft plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.2.1. This is due to the plugin storing the entire unsanitized `$_GET` superglobal array directly into the database via `update_user_meta()` when users save search results, and later outputting this data without proper escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute whenever a user accesses the saved search or views their profile, granted they can trick the user into performing the search and saving the results.	6.1	More Details
CVE-2025-66066	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EnvoThemes Envo Extra envo-extra allows Stored XSS.This issue affects Envo Extra: from n/a through <= 1.9.11.	6.1	More Details
CVE-2025-63674	An issue in Blurams Lumi Security Camera (A31C) v23.1227.472.2926 allows local physical attackers to execute arbitrary code via overriding the bootloader on the SD card.	6.1	More Details
CVE-2025-64506	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From version 1.6.0 to before 1.6.51, a heap buffer over-read vulnerability exists in libpng's png_write_image_8bit function when processing 8-bit images through the simplified write API with convert_to_8bit enabled. The vulnerability affects 8-bit grayscale+alpha, RGB/RGBA, and images with incomplete row data. A conditional guard incorrectly allows 8-bit input to enter code expecting 16-bit input, causing reads up to 2 bytes beyond allocated buffer boundaries. This issue has been patched in version 1.6.51.	6.1	More Details
CVE-2025-13134	The AuthorSure plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on the 'authorsure' 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.	6.1	More Details
CVE-2025-11885	The EchBay Admin Security plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the '_ebnonce' parameter in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-21621	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to version 2.25.0, a reflected cross-site scripting (XSS) vulnerability exists in the WMS GetFeatureInfo HTML output format that enables a remote attacker to execute arbitrary JavaScript code in a victim's browser through specially crafted SLD_BODY parameters. This issue has been patched in version 2.25.0.	6.1	More Details
CVE-2025-48987	Improper Neutralization of Input in Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes a potential reflected XSS attack.	6.1	More Details
CVE-2025-65026	esm.sh is a nobuild content delivery network(CDN) for modern web development. Prior to version 136, The esm.sh CDN service contains a Template Literal Injection vulnerability (CWE-94) in its CSS-to-JavaScript module conversion feature. When a CSS file is requested with the ?module query parameter, esm.sh converts it to a JavaScript module by embedding the CSS content directly into a template literal without proper sanitization. An attacker can inject malicious JavaScript code using ${...} expressions within CSS files, which will execute when the module is imported by victim applications. This enables Cross-Site Scripting (XSS) in browsers and Remote Code Execution (RCE) in Electron applications. This issue has been patched in version 136.	6.1	More Details

CVE-2025-63211	Stored cross-site scripting vulnerability in bridgetech VBC Server & Element Manager, firmware versions 6.5.0-9 thru 6.5.0-10, allows attackers to execute arbitrary code via the addName parameter to the /vbc/core/userSetupDoc/userSetupDoc endpoint.	6.1	More Details
CVE-2025-64027	Snipe-IT v8.3.4 (build 20218) contains a reflected cross-site scripting (XSS) vulnerability in the CSV Import workflow. When an invalid CSV file is uploaded, the application returns a progress_message value that is rendered as raw HTML in the admin interface. An attacker can intercept and modify the POST /livewire/update request to inject arbitrary HTML or JavaScript into the progress_message. Because the server accepts the modified input without sanitization and reflects it back to the user, arbitrary JavaScript executes in the browser of any authenticated admin who views the import page.	6.1	More Details
CVE-2025-36153	IBM Concert 1.0.0 through 2.0.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2025-63879	A reflected cross-site scripted (XSS) vulnerability in the /ecommerce/products.php component of E-commerce Project v1.0 and earlier allows attackers to execute arbitrary Javascript in the context of a user's browser via injecting a crafted payload into the id parameter.	6.1	More Details
CVE-2025-60796	phpPgAdmin 7.13.0 and earlier contains multiple cross-site scripting (XSS) vulnerabilities across various components. User-supplied input from $_REQUEST parameters is reflected in HTML output without proper encoding or sanitization in multiple locations including sequences.php, indexes.php, admin.php, and other unspecified files. An attacker can exploit these vulnerabilities to execute arbitrary JavaScript in victims' browsers, potentially leading to session hijacking, credential theft, or other malicious actions.	6.1	More Details
CVE-2025-63848	Stored cross site scripting (xss) vulnerability in SWISH prolog thru 2.2.0 allowing attackers to execute arbitrary code via crafted web IDE notebook.	6.1	More Details
CVE-2025-60799	phpPgAdmin 7.13.0 and earlier contains an incorrect access control vulnerability in sql.php at lines 68-76. The application allows unauthorized manipulation of session variables by accepting user-controlled parameters ('subject', 'server', 'database', 'queryid') without proper validation or access control checks. Attackers can exploit this to store arbitrary SQL queries in $_SESSION['sqlquery'] by manipulating these parameters, potentially leading to session poisoning, stored cross-site scripting, or unauthorized access to sensitive session data.	6.1	More Details
CVE-2025-64984	Kaspersky has fixed a security issue in Kaspersky Endpoint Security for Linux (any version with anti-virus databases prior to 18.11.2025), Kaspersky Industrial CyberSecurity for Linux Nodes (any version with anti-virus databases prior to 18.11.2025), and Kaspersky Endpoint Security for Mac (12.0.0.325, 12.1.0.553, and 12.2.0.694 with anti-virus databases prior to 18.11.2025) that could have allowed a reflected XSS attack to be carried out by an attacker using phishing techniques.	6.1	More Details
CVE-2025-60737	Cross Site Scripting vulnerability in Ilevia EVE X1 Server Firmware Version<= 4.7.18.0.eden:Logic Version<=6.00 - 2025_07_21 allows a remote attacker to execute arbitrary code via the /index.php component	6.1	More Details
CVE-2025-36161	IBM Concert 1.0.0 through 2.0.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict-Transport-Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2025-	IBM Concert 1.0.0 through 2.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details

36150			
CVE-2025-12394	The Backup Migration WordPress plugin before 2.0.0 does not properly generate its backup path in certain server configurations, allowing unauthenticated users to fetch a log that discloses the backup filename. The backup archive is then downloadable without authentication.	5.9	More Details
CVE-2025-64708	authentik is an open-source Identity Provider. Prior to versions 2025.8.5 and 2025.10.2, in previous authentik versions, invitations were considered valid regardless if they are expired or not, thus relying on background tasks to clean up expired ones. In a normal scenario this can take up to 5 minutes because the cleanup of expired objects is scheduled to run every 5 minutes. However, with a large amount of tasks in the backlog, this might take longer. authentik versions 2025.8.5 and 2025.10.2 fix this issue. A workaround involves creating a policy that explicitly checks whether the invitation is still valid, and then bind it to the invitation stage on the invitation flow, and denying access if the invitation is not valid.	5.8	More Details
CVE-2025-13524	Improper resource release in the call termination process in AWS Wickr before version 6.62.13 on Windows, macOS and Linux may allow a call participant to continue receiving audio input from another user after they close their call window. This issue occurs under certain conditions, which require the affected user to take a particular action within the application To mitigate this issue, users should upgrade AWS Wickr, Wickr Gov and Wickr Enterprise desktop version to version 6.62.13.	5.7	More Details
CVE-2025-33194	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause improper processing of input data. A successful exploit of this vulnerability might lead to information disclosure or denial of service.	5.7	More Details
CVE-2025-33192	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause an arbitrary memory read. A successful exploit of this vulnerability might lead to denial of service.	5.7	More Details
CVE-2025-33193	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause improper validation of integrity. A successful exploit of this vulnerability might lead to information disclosure.	5.7	More Details
CVE-2025-0007	Insufficient validation within Xilinx Run Time framework could allow a local attacker to escalate privileges from user space to kernel space, potentially compromising confidentiality, integrity, and/or availability.	5.7	More Details
CVE-2025-63952	A Cross-Site Request Forgery (CSRF) in the /mwapi?method=add-user component of Magewell Pro Convert v1.2.213 allows attackers to arbitrarily create accounts via a crafted GET request.	5.7	More Details
CVE-2025-33191	NVIDIA DGX Spark GB10 contains a vulnerability in OSROOT firmware, where an attacker could cause an invalid memory read. A successful exploit of this vulnerability might lead to denial of service.	5.7	More Details
CVE-2025-13225	Tanium addressed an arbitrary file deletion vulnerability in TanOS.	5.6	More Details
CVE-2025-13435	A security vulnerability has been detected in Dreampie Resty up to 1.3.1.SNAPSHOT. This affects the function Request of the file /resty-httpclient/src/main/java/cn/dreampie/client/HttpClient.java of the component HttpClient Module. Such manipulation of the argument filename leads to path traversal. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is reported as difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-			

2025-48511	Improper input validation within AMD uprof can allow a local attacker to write to an arbitrary physical address, potentially resulting in crash or denial of service.	5.5	More Details
CVE-2025-48502	Improper input validation within AMD uprof can allow a local attacker to overwrite MSR registers, potentially resulting in crash or denial of service.	5.5	More Details
CVE-2025-29933	Improper input validation within AMD uProf can allow a local attacker to write out of bounds, potentially resulting in a crash or denial of service	5.5	More Details
CVE-2025-31248	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Ventura 13.7.3, macOS Sequoia 15.5, macOS Sonoma 14.7.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-13467	A flaw was found in the Keycloak LDAP User Federation provider. This vulnerability allows an authenticated realm administrator to trigger deserialization of untrusted Java objects via a malicious LDAP server configuration.	5.5	More Details
CVE-2025-66063	Missing Authorization vulnerability in jgwhite33 WP Google Review Slider wp-google-places-review-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Google Review Slider: from n/a through <= 17.4.	5.4	More Details
CVE-2025-62295	SOPlanning is vulnerable to Stored XSS in /groupe_form endpoint. Malicious attacker with medium privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when opening editor. This issue was fixed in version 1.55.	5.4	More Details
CVE-2025-62296	SOPlanning is vulnerable to Stored XSS in /taches endpoint. Malicious attacker with medium privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when opening editor. This issue was fixed in version 1.55.	5.4	More Details
CVE-2025-12978	Fluent Bit in_http, in_splunk, and in_elasticsearch input plugins contain a flaw in the tag_key validation logic that fails to enforce exact key-length matching. This allows crafted inputs where a tag prefix is incorrectly treated as a full match. A remote attacker with authenticated or exposed access to these input endpoints can exploit this behavior to manipulate tags and redirect records to unintended destinations. This compromises the authenticity of ingested logs and can allow injection of forged data, alert flooding and routing manipulation.	5.4	More Details
CVE-2025-66067	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelKit Funnel Builder by FunnelKit funnel-builder allows DOM-Based XSS.This issue affects Funnel Builder by FunnelKit: from n/a through <= 3.13.1.2.	5.4	More Details
CVE-2025-62297	SOPlanning is vulnerable to Stored XSS in /projets endpoint. Malicious attacker with medium privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when opening edited page. This issue was fixed in version 1.55.	5.4	More Details
CVE-2025-66081	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Head Meta Data head-meta-data allows Stored XSS.This issue affects Head Meta Data: from n/a through <= 20250327.	5.4	More Details
CVE-2025-62729	SOPlanning is vulnerable to Stored XSS in /status endpoint. Malicious attacker with an account can inject arbitrary HTML and JS into website, which will be rendered/executed when opening multiple pages. This issue was fixed in version 1.55.	5.4	More Details
CVE-2025-11963	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saysis Computer Systems Trade Ltd. Co. StarCities allows Reflected XSS.This issue affects StarCities: before 1.1.61.	5.4	More Details
CVE-2025-	Missing Authorization vulnerability in ThemeAtelier Better Chat Support for Messenger better-chat-support allows Exploiting Incorrectly Configured Access Control Security	5.4	More

66113	Levels.This issue affects Better Chat Support for Messenger: from n/a through <= 1.2.18.		Details
CVE-2025-0504	Black Duck SCA versions prior to 2025.10.0 had user role permissions configured in an overly broad manner. Users with the scoped Project Manager user role with the Global User Read access permission enabled access to certain Project Administrator functionalities which should have be inaccessible. Exploitation does not grant full system control, but it may enable unauthorized changes to project configurations or access to system sensitive information.	5.4	More Details
CVE-2025-55127	HackerOne community member Dao Hoang Anh (yoyomiski) has reported an improper neutralization of whitespace in the username when adding new users. A username with leading or trailing whitespace could be virtually indistinguishable from its legitimate counterpart when the username is displayed in the UI, potentially leading to confusion.	5.4	More Details
CVE-2025-51662	A stored cross-site scripting (XSS) vulnerability is found in the text sharing feature of FileCodeBox version 2.2 and earlier. Insufficient input validation allows attackers to inject arbitrary JavaScript code into shared text "codeboxes". The xss payload is automatically executed in the browsers of any users who try to access the infected codebox by clicking link or entering share code.	5.4	More Details
CVE-2025-60916	A reflected cross-site scripting (XSS) vulnerability in the /overview/network/ endpoint of Austrian Archaeological Institute Openatlas before v8.12.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload into the charge parameter.	5.4	More Details
CVE-2025-13443	A vulnerability was detected in macrozheng mall up to 1.0.3. Affected by this issue is the function delete of the file /member/readHistory/delete. Performing manipulation of the argument ids results in improper access controls. Remote exploitation of the attack is possible. The exploit is now public and may be used.	5.4	More Details
CVE-2025-13468	A weakness has been identified in SourceCodester Alumni Management System 1.0. This issue affects the function delete_forum/delete_career/delete_comment/delete_gallery/delete_event of the file admin/admin_class.php of the component Delete Handler. Executing manipulation of the argument ID can lead to missing authorization. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	5.4	More Details
CVE-2025-65019	Astro is a web framework. Prior to version 5.15.9, when using Astro's Cloudflare adapter (@astrojs/cloudflare) with output: 'server', the image optimization endpoint (/_image) contains a critical vulnerability in the isRemoteAllowed() function that unconditionally allows data: protocol URLs. This enables Cross-Site Scripting (XSS) attacks through malicious SVG payloads, bypassing domain restrictions and Content Security Policy protections. This issue has been patched in version 5.15.9.	5.4	More Details
CVE-2025-13558	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'deleteUserCcDraftPost' function in all versions up to, and including, 8.7.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the status of arbitrary posts to trash.	5.4	More Details
CVE-2025-12359	The Responsive Lightbox & Gallery plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.5.3 via the 'get_image_size_by_url' function. This is due to insufficient validation of user-supplied URLs when determining image dimensions for gallery items. This makes it possible for authenticated attackers, with Author-level access and above, to make web requests to arbitrary locations originating from the web application which can be used to query and modify information from internal services.	5.4	More Details
CVE-2025-	SOPlanning is vulnerable to Broken Access Control in /status endpoint. Due to lack of permission checks in Project Status functionality an authenticated attacker is able to	5.4	More

62293	add, edit and delete any status. This issue was fixed in version 1.55.		Details
CVE-2025-12881	The Return Refund and Exchange For WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.5.5 via the wps_rma_fetch_order_msgs() due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read other user's order messages.	5.4	More Details
CVE-2025-13564	A security flaw has been discovered in SourceCodester Pre-School Management System 1.0. Impacted is the function removefile of the file app/controllers/FilehelperController.php. Performing manipulation of the argument filepath results in denial of service. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	5.4	More Details
CVE-2025-12747	The Tainacan plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.0.0 via uploaded files marked as private being exposed in wp-content without adequate protection. This makes it possible for unauthenticated attackers to extract potentially sensitive information from files that have been marked as private.	5.3	More Details
CVE-2025-58181	SSH servers parsing GSSAPI authentication requests do not validate the number of mechanisms specified in the request, allowing an attacker to cause unbounded memory consumption.	5.3	More Details
CVE-2025-64063	Primakon Pi Portal 1.0.18 API endpoints fail to enforce sufficient authorization checks when processing requests. Specifically, a standard user can exploit this flaw by sending direct HTTP requests to administrative endpoints, bypassing the UI restrictions. This allows the attacker to manipulate data outside their assigned scope, including: Unauthorized Account modification, modifying/deleting arbitrary user accounts and changing passwords by sending a direct request to the user management API endpoint; Confidential Data Access, accessing and downloading sensitive organizational documents via a direct request to the document retrieval API; Privilege escalation, This vulnerability can lead to complete compromise of data integrity and confidentiality, and Privilege Escalation by manipulating core system functions.	5.3	More Details
CVE-2025-13565	A weakness has been identified in SourceCodester Inventory Management System 1.0. The affected element is an unknown function of the file /model/user/resetPassword.php. Executing manipulation can lead to weak password recovery. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	5.3	More Details
CVE-2025-40605	A Path Traversal vulnerability has been identified in the Email Security appliance allows an attacker to manipulate file system paths by injecting crafted directory-traversal sequences (such as ../) and may access files and directories outside the intended restricted path.	5.3	More Details
CVE-2025-13318	The Booking Calendar Contact Form plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.2.60. This is due to missing authorization checks and payment verification in the `dex_bccf_check_IPN_verification` function. This makes it possible for unauthenticated attackers to arbitrarily confirm bookings and bypass payment requirements via the 'dex_bccf_ipn' parameter.	5.3	More Details
CVE-2025-47914	SSH Agent servers do not validate the size of messages when processing new identity requests, which may cause the program to panic if the message is malformed due to an out of bounds read.	5.3	More Details
CVE-2025-	The Appointment Booking Calendar plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.3.96. This is due to the plugin exposing an unauthenticated booking processing endpoint (cpabc_appointments_check_IPN_verification) that trusts attacker-supplied payment notifications without verifying their origin, authenticity, or requiring proper	5.3	More Details

13317	authorization checks. This makes it possible for unauthenticated attackers to arbitrarily confirm bookings and insert them into the live calendar via the 'cpabc_ipncheck' parameter, triggering administrative and customer notification emails and disrupting operations.		
CVE-2025-29934	A bug within some AMD CPUs could allow a local admin-privileged attacker to run a SEV-SNP guest using stale TLB entries, potentially resulting in loss of data integrity.	5.3	More Details
CVE-2025-13147	Server-Side Request Forgery (SSRF) vulnerability in Progress MOVEit Transfer.This issue affects MOVEit Transfer: before 2024.1.8, from 2025.0.0 before 2025.0.4.	5.3	More Details
CVE-2025-12877	The IDonate – Blood Donation, Request And Donor Management System plugin for WordPress is vulnerable to unauthorized modification od data due to a missing capability check on the panding_blood_request_action() function in all versions up to, and including, 2.1.15. This makes it possible for unauthenticated attackers to delete arbitrary posts.	5.3	More Details
CVE-2025-12752	The Subscriptions & Memberships for PayPal plugin for WordPress is vulnerable to fake payment creation in all versions up to, and including, 1.1.7. This is due to the plugin not properly verifying the authenticity of an IPN request. This makes it possible for unauthenticated attackers to create fake payment entries that have not actually occurred.	5.3	More Details
CVE-2025-64067	Primakon Pi Portal 1.0.18 API endpoints responsible for retrieving object-specific or filtered data (e.g., user profiles, project records) fail to implement sufficient server-side validation to confirm that the requesting user is authorized to access the requested object or dataset. This vulnerability can be exploited in two ways: Direct ID manipulation and IDOR, by changing an ID parameter (e.g., user_id, project_id) in the request, an attacker can access the object and data belonging to another user; and filter Omission, by omitting the filtering parameter entirely, an attacker can cause the endpoint to return an entire unfiltered dataset of all stored records for all users. This flaw leads to the unauthorized exposure of sensitive personal and organizational information.	5.3	More Details
CVE-2025-12525	The Locker Content plugin for WordPress is vulnerable to Sensitive Information Exposure in version 1.0.0 via the 'lockerco_submit_post' AJAX endpoint. This makes it possible for unauthenticated attackers to extract content from posts that has been protected by the plugin.	5.3	More Details
CVE-2025-12043	The Autochat Automatic Conversation plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_nopriv_auycht_saveCid' AJAX endpoint in all versions up to, and including, 1.1.9. This makes it possible for unauthenticated attackers to connect and disconnect the client ID.	5.3	More Details
CVE-2025-64765	Astro is a web framework. Prior to version 5.15.8, a mismatch exists between how Astro normalizes request paths for routing/rendering and how the application’s middleware reads the path for validation checks. Astro internally applies decodeURI() to determine which route to render, while the middleware uses context.url.pathname without applying the same normalization (decodeURI). This discrepancy may allow attackers to reach protected routes using encoded path variants that pass routing but bypass validation checks. This issue has been patched in version 5.15.8.	5.3	More Details
CVE-2025-66099	Missing Authorization vulnerability in ThemeAtelier Chat Help chat-help allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Chat Help: from n/a through <= 3.1.3.	5.3	More Details
CVE-	The Ultimate Member Widgets for Elementor – WordPress User Directory plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability		

2025-12778	check on the handle_filter_users function in all versions up to, and including, 2.3. This makes it possible for unauthenticated attackers to extract partial metadata of all WordPress users, including their first name, last name and email addresses.	5.3	More Details
CVE-2025-13434	A weakness has been identified in jameschz Hush Framework 2.0. The impacted element is an unknown function of the file Hush\hush-lib\hush\Util.php of the component HTTP Host Header Handler. This manipulation of the argument $_SERVER['HOST'] causes improper neutralization of http headers for scripting syntax. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-12814	The SiteSEO – SEO Simplified plugin for WordPress is vulnerable to unauthorized modification of data due to n incorrect capability check on the siteseo_reset_settings function in all versions up to, and including, 1.3.2. This makes it possible for authenticated attackers, who have been granted access to at least on SiteSEO setting capability, to reset the plugin's settings.	5.3	More Details
CVE-2025-66064	Cross-Site Request Forgery (CSRF) vulnerability in Syed Balkhi Giveaways and Contests by RafflePress rafflepress allows Cross Site Request Forgery.This issue affects Giveaways and Contests by RafflePress: from n/a through <= 1.12.20.	5.3	More Details
CVE-2025-12777	The YITH WooCommerce Wishlist plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.10.0. This is due to the plugin not properly verifying that a user is authorized to perform actions on the REST API /wp-json/yith/wishlist/v1/lists endpoint (which uses permission_callback => '__return_true') and the AJAX delete_item handler (which only checks nonce validity without verifying object-level authorization). This makes it possible for unauthenticated attackers to disclose wishlist tokens for any user and subsequently delete wishlist items by chaining the REST API authorization bypass with the exposed delete_item nonce on shared wishlist pages and the AJAX handler's missing object-level authorization check.	5.3	More Details
CVE-2025-13405	The Ace Post Type Builder plugin for WordPress is vulnerable to unauthorized custom taxonomy deletion due to missing authorization validation on the cptb_delete_custom_taxonomy() function in all versions up to, and including, 1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary custom taxonomies.	5.3	More Details
CVE-2025-12535	The SureForms plugin for WordPress is vulnerable to Cross-Site Request Forgery Bypass in all versions up to, and including, 1.13.1. This is due to the plugin distributing generic WordPress REST API nonces (wp_rest) to unauthenticated users via the 'wp_ajax_nopriv_rest-nonce' action. While the plugin legitimately needs to support unauthenticated form submissions, it incorrectly uses generic REST nonces instead of form-specific nonces. This makes it possible for unauthenticated attackers to bypass CSRF protection on REST API endpoints that rely solely on nonce verification without additional authentication checks, allowing them to trigger unauthorized actions such as the plugin's own post-submission hooks and potentially other plugins' REST endpoints.	5.3	More Details
CVE-2025-56423	An issue in Austrian Academy of Sciences (AW) Austrian Archaeological Institute OpenAtlas v.8.12.0 allows a remote attacker to obtain sensitive information via the login error messages	5.3	More Details
CVE-2025-12842	The Booking Plugin for WordPress Appointments – Time Slot plugin for WordPress is vulnerable to unauthorized email sending in versions up to, and including, 1.4.7 due to missing validation on the tslot_appt_email AJAX action. This makes it possible for unauthenticated attackers to send appointment notification emails to arbitrary recipients with attacker-controlled text content in certain email fields, potentially enabling the site to be abused for phishing campaigns or spam distribution.	5.3	More Details
CVE-2025-	Missing Authorization vulnerability in Jegstudio Gutenverse gutenverse allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects	5.3	More

66065	Gutenverse: from n/a through <= 3.2.1.		Details
CVE-2025-12894	The Import WP – Export and Import CSV and XML files to WordPress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.14.17 via the import/export functionality and a lack of .htaccess protection. This makes it possible for unauthenticated attackers to extract sensitive data from exports stored in /exportwp and import data stored in /importwp.	5.3	More Details
CVE-2025-12770	The New User Approve plugin for WordPress is vulnerable to unauthorized data disclosure in all versions up to, and including, 3.0.9 due to insufficient API key validation using loose equality comparison. This makes it possible for unauthenticated attackers to retrieve personally identifiable information (PII), including usernames and email addresses of users with various approval statuses via the Zapier REST API endpoints, by exploiting PHP type juggling with the api_key parameter set to "0" on sites where the Zapier API key has not been configured.	5.3	More Details
CVE-2025-66060	Missing Authorization vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Seriously Simple Podcasting: from n/a through <= 3.13.0.	5.3	More Details
CVE-2025-66059	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Retrieve Embedded Sensitive Data.This issue affects Seriously Simple Podcasting: from n/a through <= 3.13.0.	5.3	More Details
CVE-2025-12039	The BigBuy Dropshipping Connector for WooCommerce plugin for WordPress is vulnerable to IP Address Spoofing in all versions up to, and including, 2.0.5 due to insufficient IP address validation and use of user-supplied HTTP headers as a primary method for IP retrieval. This makes it possible for unauthenticated attackers to retrieve the output of phpinfo().	5.3	More Details
CVE-2025-12426	The Quiz Maker plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.7.0.80. This is due to the plugin exposing quiz answers through the ays_quiz_check_answer AJAX action without proper authorization checks. The endpoint only validates a nonce, but that same nonce is publicly available to all site visitors via the quiz_maker_ajax_public localized script data. This makes it possible for unauthenticated attackers to extract sensitive data including quiz answers for any quiz question.	5.3	More Details
CVE-2025-36160	IBM Concert 1.0.0 through 2.0.0 could disclose sensitive server information from HTTP response headers that could aid in further attacks against the system.	5.3	More Details
CVE-2025-10054	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'eh_crm_remove_agent' function in all versions up to, and including, 3.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to remove the role and capabilities of any user with an Administrator, WSDesk Supervisor, or WSDesk Agents role.	5.3	More Details
CVE-2025-12972	Fluent Bit out_file plugin does not properly sanitize tag values when deriving output file names. When the File option is omitted, the plugin uses untrusted tag input to construct file paths. This allows attackers with network access to craft tags containing path traversal sequences that cause Fluent Bit to write files outside the intended output directory.	5.3	More Details
CVE-2025-13414	The Chamber Dashboard Business Directory plugin for WordPress is vulnerable to unauthorized data export due to a missing capability check on the cdash_watch_for_export() function in all versions up to, and including, 3.3.11. This makes it possible for unauthenticated attackers to export business directory	5.3	More Details

	information, including sensitive business details.		
CVE-2025-13386	The Social Images Widget plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'options_update' function in all versions up to, and including, 2.1. This makes it possible for unauthenticated attackers to delete 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.	5.3	More Details
CVE-2025-66087	Missing Authorization vulnerability in Property Hive PropertyHive propertyhive allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PropertyHive: from n/a through <= 2.1.12.	5.3	More Details
CVE-2025-12349	The Icegram Express - Email Subscribers, Newsletters and Marketing Automation Plugin for WordPress is vulnerable to Authorization in versions up to, and including, 5.9.10. This is due to the plugin not properly verifying that a user is authorized to perform an action in the `trigger_mailing_queue_sending` function. This makes it possible for unauthenticated attackers to force immediate email sending, bypass the schedule, increase server load, and change plugin state (e.g., last-cron-hit), enabling abuse or DoS-like effects.	5.3	More Details
CVE-2025-11368	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Sensitive Information Disclosure in all versions up to, and including, 4.2.9.4. This is due to missing capability checks in the REST endpoint /wp-json/lp/v1/load_content_via_ajax which allows arbitrary callback execution of admin-only template methods. This makes it possible for unauthenticated attackers to retrieve admin curriculum HTML, quiz questions with correct answers, course materials, and other sensitive educational content via the REST API endpoint granted they can supply valid numeric IDs.	5.3	More Details
CVE-2025-12427	The YITH WooCommerce Wishlist plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.10.0 via the REST API endpoint and AJAX handler due to missing validation on user-controlled keys. This makes it possible for unauthenticated attackers to discover any user's wishlist token ID, and subsequently rename the victim's wishlist without authorization (integrity impact). This can be exploited to target multi-user stores for defacement, social engineering attacks, mass tampering, and profiling at scale.	5.3	More Details
CVE-2025-36112	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7 and 6.2.0.0 through 6.2.0.5 and 6.2.1.1 could reveal sensitive server IP configuration information to an unauthorized user.	5.3	More Details
CVE-2025-13404	The atec Duplicate Page & Post plugin for WordPress is vulnerable to unauthorized post duplication due to missing authorization validation on the duplicate_post() function in all versions up to, and including, 1.2.20. This makes it possible for authenticated attackers, with Contributor-level access and above, to duplicate arbitrary posts, including private and password-protected posts, leading to data exposure.	5.3	More Details
CVE-2025-11771	The Cryptocurrency (Token), Launchpad (Presale), ICO & IDO, Airdrop by TokenICO plugin for WordPress is vulnerable to unauthenticated and unauthorized modification of data due to missing authentication and capability checks on the 'createSaleRecord' function in all versions up to, and including, 2.4.6. This makes it possible for unauthenticated attackers to manipulate presales counters.	5.3	More Details
CVE-2025-13389	The Admin and Customer Messages After Order for WooCommerce: OrderConvo plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the `get_order_by_id()` function in all versions up to, and including, 14. This makes it possible for unauthenticated attackers to view sensitive WooCommerce order details and private conversation messages between customers and store administrators for any order by supplying an arbitrary order ID.	5.3	More Details
CVE-2025-	A vulnerability was found in the Application Server of Desktop Alert PingAlert version	5.3	More

54341	6.1.0.11 to 6.1.1.2. There are Hard-coded configuration values.		Details
CVE-2025-12170	The Checkbox plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'wp_ajax_nopriv_checkbox_clean_log' AJAX endpoint in all versions up to, and including, 2.8.10. This makes it possible for unauthenticated attackers to clear log files.	5.3	More Details
CVE-2025-66086	Missing Authorization vulnerability in Cozy Vision SMS Alert Order Notifications sms-alert allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SMS Alert Order Notifications: from n/a through <= 3.8.8.	5.3	More Details
CVE-2025-64713	WebAssembly Micro Runtime (WAMR) is a lightweight standalone WebAssembly (Wasm) runtime. Prior to version 2.4.4, an out-of-bounds array access issue exists in WAMR's fast interpreter mode during WASM bytecode loading. When frame_ref_bottom and frame_offset_bottom arrays are at capacity and a GET_GLOBAL(I32) opcode is encountered, frame_ref_bottom is expanded but frame_offset_bottom may not be. If this is immediately followed by an if opcode that triggers preserve_local_for_block, the function traverses arrays using stack_cell_num as the upper bound, causing out-of-bounds access to frame_offset_bottom since it wasn't expanded to match the increased stack_cell_num. This issue has been patched in version 2.4.4.	5.1	More Details
CVE-2025-36158	IBM Concert 1.0.0 through 2.0.0 could allow a local user with specific permission to obtain sensitive information from files due to uncontrolled recursive directory copying.	5.1	More Details
CVE-2025-9825	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.7 to 18.2.8, 18.3 before 18.3.4, and 18.4 before 18.4.2 that could have allowed authenticated users without project membership to view sensitive manual CI/CD variables by querying the GraphQL API.	5.0	More Details
CVE-2025-12766	An Insecure Direct Object Reference (IDOR) vulnerability in the Management Console of BlackBerry® AtHoc® (OnPrem) version 7.21 could allow an attacker to potentially gain unauthorized knowledge about other organizations hosted on the same Interactive Warning System (IWS).	5.0	More Details
CVE-2025-13370	The ProjectList plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 0.3.0 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 Editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-11973	The 简数采集器 plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 2.6.3 via the __kds_flag functionality that imports featured images. This makes it possible for authenticated attackers, with Adminstrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2025-12750	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to SQL Injection via the 'term' parameter in all versions up to, and including, 4.2.6.1 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, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-13385	The Bookme – Free Online Appointment Booking and Scheduling Plugin for WordPress is vulnerable to time-based SQL Injection via the `filter[status]` parameter in all versions up to, and including, 4.2 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 admin-level access and above, to append additional SQL	4.9	More Details

	queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2025-64049	A stored cross-site scripting (XSS) vulnerability in the module management component in REDAXO CMS 5.20.0 allows remote users to inject arbitrary web script or HTML via the Output code field in modules. The payload is executed when a user views or edits an article by adding slice that uses the compromised module.	4.8	More Details
CVE-2025-64521	authentik is an open-source Identity Provider. Prior to versions 2025.8.5 and 2025.10.2, when authenticating with client_id and client_secret to an OAuth provider, authentik creates a service account for the provider. In previous authentik versions, authentication for this account was possible even when the account was deactivated. Other permissions are correctly applied and federation with other providers still take assigned policies correctly into account. authentik versions 2025.8.5 and 2025.10.2 fix this issue. A workaround involves adding a policy to the application that explicitly checks if the service account is still valid, and deny access if not.	4.8	More Details
CVE-2025-62731	SOPlanning is vulnerable to Stored XSS in /feries endpoint. Malicious attacker with access to public holidays feature is able to inject arbitrary HTML and JS into website, which will be rendered/executed when opening multiple pages. By default only administrators and users with special privileges are able to access this endpoint. This issue was fixed in version 1.55.	4.8	More Details
CVE-2025-13545	A security vulnerability has been detected in ashraf-kabir travel-agency up to 1f25aa03544bc5fb7a9e846f8a7879cecdb0cad3. Affected by this vulnerability is an unknown functionality of the file /admin_area/index.php. The manipulation of the argument edit_pack leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-13411	A vulnerability was found in Campcodes Retro Basketball Shoes Online Store 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin_football.php. Performing manipulation of the argument product_image results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-13574	A weakness has been identified in code-projects Online Bidding System 1.0. This issue affects the function categoryadd of the file /administrator/addcategory.php. This manipulation of the argument catimage causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-64704	WebAssembly Micro Runtime (WAMR) is a lightweight standalone WebAssembly (Wasm) runtime. Prior to version 2.4.4, WAMR is susceptible to a segmentation fault in v128.store instruction. This issue has been patched in version 2.4.4.	4.7	More Details
CVE-2025-13423	A flaw has been found in Campcodes Retro Basketball Shoes Online Store 1.0. The impacted element is an unknown function of the file /admin/admin_product.php. Executing manipulation of the argument product_image can lead to unrestricted upload. The attack may be launched remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2025-12569	The Guest posting / Frontend Posting / Front Editor WordPress plugin before 5.0.0 does not validate a parameter before redirecting the user to its value, leading to an Open Redirect issue	4.7	More Details
CVE-2025-0421	Improper Restriction of Rendered UI Layers or Frames vulnerability in Shopside Software Technologies Inc. Shopside allows iFrame Overlay.This issue affects Shopside: through 05022025.	4.7	More Details

CVE-2025-58412	A improper neutralization of script-related html tags in a web page (basic xss) vulnerability in Fortinet FortiADC 8.0.0, FortiADC 7.6.0 through 7.6.3, FortiADC 7.4 all versions, FortiADC 7.2 all versions may allow attacker to execute unauthorized code or commands via crafted URL.	4.7	More Details
CVE-2025-13586	A flaw has been found in SourceCodester Online Student Clearance System 1.0. Impacted is an unknown function of the file /Admin/changepassword.php. This manipulation of the argument txtconfirm_password causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2025-13424	A vulnerability has been found in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_product.php. The manipulation of the argument txtProductName leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-63433	Xtooltech Xtool AnyScan Android Application 4.40.40 and prior uses a hardcoded cryptographic key and IV to decrypt update metadata. The key is stored as a static value within the application's code. An attacker with the ability to intercept network traffic can use this hardcoded key to decrypt, modify, and re-encrypt the update manifest, allowing them to direct the application to download a malicious update package.	4.6	More Details
CVE-2025-60917	A reflected cross-site scripting (XSS) vulnerability in the /overview/network/ endpoint of Austrian Archaeological Institute Openatlas before v8.12.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload into the color parameter.	4.6	More Details
CVE-2025-60914	Incorrect access control in Austrian Archaeological Institute Openatlas before v8.12.0 allows attackers to access sensitive information via sending a crafted GET request to the /display_logo endpoint.	4.6	More Details
CVE-2025-63432	Xtooltech Xtool AnyScan Android Application 4.40.40 and prior is Missing SSL Certificate Validation. The application fails to properly validate the TLS certificate from its update server. An attacker on the same network can exploit this vulnerability by performing a Man-in-the-Middle (MITM) attack to intercept, decrypt, and modify traffic between the application and the update server. This serves as the basis for further attacks, including Remote Code Execution.	4.6	More Details
CVE-2025-63243	A reflected cross-site scripting (XSS) vulnerability exists in the password change functionality of Pixeon WebLaudos 25.1 (01). The sle_sSenha parameter to the loginAlterarSenha.asp file. An attacker can craft a malicious URL that, when visited by a victim, causes arbitrary JavaScript code to be executed in the victim's browser within the security context of the vulnerable application. This issue could allow attackers to steal session cookies, disclose sensitive information, perform unauthorized actions on behalf of the user, or conduct phishing attacks.	4.6	More Details
CVE-2025-12066	The WP Delete Post Copies plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 6.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-33195	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause unexpected memory buffer operations. A successful exploit of this vulnerability might lead to data tampering, denial of service, or escalation of privileges.	4.4	More Details
CVE-	The YouTube Subscribe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated		

2025-12025	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.	4.4	More Details
CVE-2025-13311	The Just Highlight plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Highlight Color' setting in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the plugin's settings page.	4.4	More Details
CVE-2025-33196	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause a resource to be reused. A successful exploit of this vulnerability might lead to information disclosure.	4.4	More Details
CVE-2025-12032	The Zweb Social Mobile – Ứng Dụng Nút Gọi Mobile plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘vithanhlam_zsocial_save_messager’, 'vithanhlam_zsocial_save_zalo', 'vithanhlam_zsocial_save_hotline', and 'vithanhlam_zsocial_save_contact' parameters in all versions up to, and including, 1.0.0 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.	4.4	More Details
CVE-2025-33197	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause a NULL pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	4.3	More Details
CVE-2025-65502	Null pointer dereference in add_ca_certs() in Cesanta Mongoose before 7.2 allows remote attackers to cause a denial of service via TLS initialization where SSL_CTX_get_cert_store() returns NULL.	4.3	More Details
CVE-2025-63435	Xtooltech Xtool AnyScan Android Application 4.40.40 is Missing Authentication for Critical Function. The server-side endpoint responsible for serving update packages for the application does not require any authentication. This allows an unauthenticated remote attacker to freely download official update packages..	4.3	More Details
CVE-2025-12751	The WSChat – WordPress Live Chat plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'reset_settings' AJAX endpoint in all versions up to, and including, 3.1.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the plugin's settings.	4.3	More Details
CVE-2025-65501	Null pointer dereference in coap_dtls_info_callback() in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a DTLS handshake where SSL_get_app_data() returns NULL.	4.3	More Details
CVE-2025-10646	The Search Exclude plugin for WordPress is vulnerable to unauthorized modification of data due to a insufficient capability check on the Base::get_rest_permission() method in all versions up to, and including, 2.5.7. This makes it possible for authenticated attackers, with Contributor-level access and above, to modify plugin settings, such as adding arbitrary posts to the search exclusion list.	4.3	More Details
CVE-2025-12822	The WP Login and Register using JWT plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'mo_jwt_generate_new_api_key' function in all versions up to, and including, 3.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to generate a new API key on site's that do not have an API key configured and subsequently use that to access restricted endpoints.	4.3	More Details
	The SiteSEO – SEO Simplified plugin for WordPress is vulnerable to Improper		

CVE-2025-13085	Authorization leading to Sensitive Post Meta Disclosure in versions up to and including 1.3.2. This is due to missing object-level authorization checks in the resolve_variables() AJAX handler. This makes it possible for authenticated attackers with the siteseo_manage capability (e.g., Author-level users who have been granted SiteSEO access by an administrator) to read arbitrary post metadata from any post, page, attachment, or WooCommerce order they cannot edit, via the custom field variable resolution feature granted they have been given access to SiteSEO by an administrator and legacy storage is enabled. In affected WooCommerce installations, this exposes sensitive customer billing information including names, email addresses, phone numbers, physical addresses, and payment methods.	4.3	More Details
CVE-2025-65647	Insecure Direct Object Reference (IDOR) in the Track order function in PHPGURUKUL Online Shopping Portal 2.1 allows information disclosure via the oid parameter.	4.3	More Details
CVE-2025-65496	NULL pointer dereference in coap_dtls_generate_cookie() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted DTLS handshake that triggers SSL_get_SSL_CTX() to return NULL.	4.3	More Details
CVE-2025-65497	NULL pointer dereference in coap_dtls_generate_cookie() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted DTLS handshake that triggers SSL_get_SSL_CTX() to return NULL.	4.3	More Details
CVE-2025-65498	NULL pointer dereference in coap_dtls_generate_cookie() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted DTLS handshake that triggers SSL_get_SSL_CTX() to return NULL.	4.3	More Details
CVE-2025-65499	Array index error in tls_verify_call_back() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted DTLS handshake that triggers SSL_get_ex_data_X509_STORE_CTX_idx() to return -1.	4.3	More Details
CVE-2025-65500	NULL pointer dereference in coap_dtls_generate_cookie() in src/coap_openssl.c in OISM libcoap 4.3.5 allows remote attackers to cause a denial of service via a crafted DTLS handshake that triggers SSL_get_SSL_CTX() to return NULL.	4.3	More Details
CVE-2025-11773	The Cryptocurrency (Token), Launchpad (Presale), ICO & IDO, Airdrop by TokenICO plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'saveDeployedContract' function in all versions up to, and including, 2.4.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the WordPress option `tokenico_deployed_contracts`, poisoning the smart contract addresses displayed.	4.3	More Details
CVE-2025-65226	Tenda AC21 V16.03.08.16 is vulnerable to Buffer Overflow via the deviceId parameter in /goform/saveParentControlInfo.	4.3	More Details
CVE-2025-62724	Open OnDemand is an open-source HPC portal. Prior to versions 4.0.8 and 3.1.16, users can craft a "Time of Check to Time of Use" (TOCTOU) attack when downloading zip files to access files outside of the OOD_ALLOWLIST. This vulnerability impacts sites that use the file browser allowlists in all current versions of OOD. However, files accessed are still protected by the UNIX permissions. Open OnDemand versions 4.0.8 and 3.1.16 have been patched for this vulnerability.	4.3	More Details
CVE-2025-66089	Missing Authorization vulnerability in WebToffee Product Feed for WooCommerce webtoffee-product-feed allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Product Feed for WooCommerce: from n/a through <= 2.3.1.	4.3	More Details
CVE-2025-66069	Missing Authorization vulnerability in Themeisle PPOM for WooCommerce woocommerce-product-addon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PPOM for WooCommerce: from n/a through <= 33.0.16.	4.3	More Details

CVE-2025-66077	Missing Authorization vulnerability in wpWax Legal Pages legal-pages allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Legal Pages: from n/a through <= 1.4.6.	4.3	More Details
CVE-2025-64061	Primakon Pi Portal 1.0.18 /api/v2/users endpoint is vulnerable to unauthorized data exposure due to deficient access control mechanisms. Any authenticated user, regardless of their privilege level (including standard or low-privileged users), can make a GET request to this endpoint and retrieve a complete, unfiltered list of all registered application users. Crucially, the API response body for this endpoint includes password hashes.	4.3	More Details
CVE-2025-66082	Missing Authorization vulnerability in magepeopleteam WpEvently mage-eventpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WpEvently: from n/a through <= 5.0.4.	4.3	More Details
CVE-2025-66083	Missing Authorization vulnerability in magepeopleteam WpEvently mage-eventpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WpEvently: from n/a through <= 5.0.4.	4.3	More Details
CVE-2025-66084	Missing Authorization vulnerability in Shahjahan Jewel FluentCommunity fluent-community allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FluentCommunity: from n/a through <= 2.0.0.	4.3	More Details
CVE-2025-66085	Missing Authorization vulnerability in tychesoftwares Arconix Shortcodes arconix-shortcodes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Arconix Shortcodes: from n/a through <= 2.1.18.	4.3	More Details
CVE-2025-66097	Cross-Site Request Forgery (CSRF) vulnerability in Igor Jerosimić I Order Terms i-order-terms allows Cross Site Request Forgery.This issue affects I Order Terms: from n/a through <= 1.5.0.	4.3	More Details
CVE-2025-66061	Cross-Site Request Forgery (CSRF) vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Cross Site Request Forgery.This issue affects Seriously Simple Podcasting: from n/a through <= 3.13.0.	4.3	More Details
CVE-2025-66101	Missing Authorization vulnerability in Sabuj Kundu CBX Bookmark & Favorite cbxwpbookmark allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CBX Bookmark & Favorite: from n/a through <= 2.0.1.	4.3	More Details
CVE-2025-13382	The Frontend File Manager Plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 23.4. This is due to the plugin not validating file ownership before processing file rename requests in the '/wpfm/v1/file-rename' REST API endpoint. This makes it possible for authenticated attackers, with Subscriber-level access and above, to rename files uploaded by other users via the 'fileid' parameter.	4.3	More Details
CVE-2025-66112	Missing Authorization vulnerability in WebToffee Accessibility Toolkit by WebYes accessibility-plus allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Accessibility Toolkit by WebYes: from n/a through <= 2.0.4.	4.3	More Details
CVE-2025-43374	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iPadOS 17.7.7, iOS 18.5 and iPadOS 18.5, visionOS 2.5, macOS Sonoma 14.7.3, macOS Ventura 13.7.3, macOS Sequoia 15.5, watchOS 11.5. An attacker in physical proximity may be able to cause an out-of-bounds read in kernel memory.	4.3	More Details
CVE-2025-13432	Terraform state versions can be created by a user with specific but insufficient permissions in a Terraform Enterprise workspace. This may allow for the alteration of infrastructure if a subsequent plan operation is approved by a user with approval permission or auto-applied. This vulnerability, CVE-2025-13432, is fixed in Terraform Enterprise version 1.1.1 and 1.0.3.	4.3	More Details
CVE-	A spoofing issue was addressed with improved truncation when displaying the fully		More

2025-31266	qualified domain name This issue is fixed in Safari 18.5, macOS Sequoia 15.5. A website may be able to spoof the domain name in the title of a pop-up window.	4.3	Details
CVE-2025-12634	The Refund Request for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_refund_status' function in all versions up to, and including, 1.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update refund statuses to approved or rejected.	4.3	More Details
CVE-2025-12586	The Conditional Maintenance Mode for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing nonce validation when toggling the maintenance mode status. This makes it possible for unauthenticated attackers to enable or disable the site's maintenance mode via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12587	The Peer Publish plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the website management pages. This makes it possible for unauthenticated attackers to add, modify, or delete website configurations via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-11815	The UiPress lite | Effortless custom dashboards, admin themes and pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the uip_save_site_option() function in all versions up to, and including, 3.5.08. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary plugin settings. Other AJAX actions are also affected.	4.3	More Details
CVE-2025-13136	The GSheetConnector For Ninja Forms plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'njform-google-sheet-config ' page in all versions up to, and including, 2.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve information about the system.	4.3	More Details
CVE-2025-12086	The Return Refund and Exchange For WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.5.5 via the 'wps_rma_cancel_return_request' AJAX endpoint due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete other users refund requests.	4.3	More Details
CVE-2025-65220	Tenda AC21 V16.03.08.16 is vulnerable to Buffer Overflow in: /goform/SetVirtualServerCfg via the list parameter.	4.3	More Details
CVE-2025-65221	Tenda AC21 V16.03.08.16 is vulnerable to Buffer Overflow via the list parameter of /goform/setPptpUserList.	4.3	More Details
CVE-2025-12169	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_eh_crm_settings_empty_scheduled_actions' AJAX Action in all versions up to, and including, 3.3.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear the scheduled triggers option.	4.3	More Details
CVE-2025-65222	Tenda AC21 V16.03.08.16 is vulnerable to Buffer Overflow via the rebootTime parameter of /goform/SetSysAutoRebbotCfg.	4.3	More Details
CVE-2025-	The Custom Post Type plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the custom post type deletion functionality. This makes it possible for unauthenticated	4.3	More

13142	attackers to delete custom post types via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		Details
CVE-2025-12085	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'eh_crm_settings_empty_trash' function in all versions up to, and including, 3.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to empty the ticket trash.	4.3	More Details
CVE-2025-12023	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the eh_crm_restore_data() function in all versions up to, and including, 3.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to restore tickets.	4.3	More Details
CVE-2025-12022	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'eh_crm_settings_restore_trash' AJAX endpoint in all versions up to, and including, 3.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to restore all deleted tickets.	4.3	More Details
CVE-2025-13149	The Schedule Post Changes With PublishPress Future: Unpublish, Delete, Change Status, Trash, Change Categories plugin for WordPress is vulnerable to unauthorized modification of data due to a missing authorization check on the "saveFutureActionData" function in all versions up to, and including, 4.9.1. This makes it possible for authenticated attackers, with author level access and above, to change the status of arbitrary posts and pages via the REST API endpoint.	4.3	More Details
CVE-2025-13452	The Admin and Customer Messages After Order for WooCommerce: OrderConvo plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 14. This is due to a flawed permission check in the REST API permission callback that returns true when no nonce is provided. This makes it possible for unauthenticated attackers to impersonate any WordPress user and inject arbitrary messages into any WooCommerce order conversation by directly calling the REST endpoint with controlled user_id, order_id, and context parameters.	4.3	More Details
CVE-2025-10039	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.2.9 via the 'eh_crm_ticket_single_view_client' due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of all support tickets.	4.3	More Details
CVE-2025-66056	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Uncanny Owl Uncanny Automator uncanny-automator allows Retrieve Embedded Sensitive Data.This issue affects Uncanny Automator: from n/a through < 6.10.0.	4.3	More Details
CVE-2025-65223	Tenda AC21 V16.03.08.16 is vulnerable to Buffer Overflow via the urls parameter of /goform/saveParentControlInfo.	4.3	More Details
CVE-2025-12893	Clients may successfully perform a TLS handshake with a MongoDB server despite presenting a client certificate not aligning with the documented Extended Key Usage (EKU) requirements. A certificate that specifies extendedKeyUsage but is missing extendedKeyUsage = clientAuth may still be successfully authenticated via the TLS handshake as a client. This issue is specific to MongoDB servers running on Windows or Apple as the expected validation behavior functions correctly on Linux systems. Additionally, MongoDB servers may successfully establish egress TLS connections with servers that present server certificates not aligning with the documented Extended Key Usage (EKU) requirements. A certificate that specifies extendedKeyUsage but is missing extendedKeyUsage = serverAuth may still be successfully authenticated via	4.2	More Details

	the TLS handshake as a server. This issue is specific to MongoDB servers running on Apple as the expected validation behavior functions correctly on both Linux and Windows systems. This vulnerability affects MongoDB Server v7.0 versions prior to 7.0.26, MongoDB Server v8.0 versions prior to 8.0.16 and MongoDB Server v8.2 versions prior to 8.2.2		
CVE-2025-66075	Missing Authorization vulnerability in WP Legal Pages WP Cookie Notice for GDPR, CCPA & ePrivacy Consent gdpr-cookie-consent allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Cookie Notice for GDPR, CCPA & ePrivacy Consent: from n/a through <= 4.0.3.	4.2	More Details
CVE-2025-36134	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7 and 6.2.0.0 through 6.2.0.5 and 6.2.1.1 could disclose sensitive information due to a missing or insecure SameSite attribute for a sensitive cookie.	3.7	More Details
CVE-2025-66062	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Frank Goossens WP YouTube Lyte wp-youtube-lyte allows Phishing.This issue affects WP YouTube Lyte: from n/a through <= 1.7.28.	3.7	More Details
CVE-2025-35029	Medical Informatics Engineering Enterprise Health has a stored cross site scripting vulnerability that allows an authenticated attacker to add arbitrary content in the 'Demographic Information' page. This content will be rendered and executed when a victim accesses it. This issue is fixed as of 2025-03-14.	3.5	More Details
CVE-2025-13450	A vulnerability was determined in SourceCodester Online Shop Project 1.0. Impacted is an unknown function of the file /shop/register.php. This manipulation of the argument f_name causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	3.5	More Details
CVE-2025-13415	A vulnerability was identified in icret EasyImages up to 2.8.6. This affects an unknown part of the file /app/upload.php of the component SVG Image Handler. The manipulation of the argument File leads to cross site scripting. It is possible to initiate the attack remotely.	3.5	More Details
CVE-2025-64757	Astro is a web framework. Prior to version 5.14.3, a vulnerability has been identified in the Astro framework's development server that allows arbitrary local file read access through the image optimization endpoint. The vulnerability affects Astro development environments and allows remote attackers to read any image file accessible to the Node.js process on the host system. This issue has been patched in version 5.14.3.	3.5	More Details
CVE-2025-13584	A security vulnerability has been detected in Eigenfocus up to 1.4.0. This vulnerability affects unknown code of the component Description Handler. The manipulation of the argument entry.description/time_entry.description leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 1.4.1 is able to resolve this issue. The identifier of the patch is 7dec94c9d1f3e513e0ee38ba68caaba628e08582. Upgrading the affected component is advised.	3.5	More Details
CVE-2025-13577	A flaw has been found in PHPGurukul Hostel Management System 2.1. The impacted element is an unknown function of the file /register-complaint.php. Executing manipulation of the argument cdetails can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	3.5	More Details
CVE-2025-13397	A security vulnerability has been detected in mrubyc up to 3.4. This impacts the function mrbc_raw_realloc of the file src/alloc.c. Such manipulation of the argument ptr leads to null pointer dereference. An attack has to be approached locally. The name of the patch is 009111904807b8567262036bf45297c3da8f1c87. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2025-33198	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause a resource to be reused. A successful exploit of this vulnerability might lead to information disclosure.	3.3	More Details

CVE-2025-13566	A security vulnerability has been detected in jarun nnn up to 5.1. The impacted element is the function show_content_in_floating_window/run_cmd_as_plugin of the file nnn/src/nnn.c. The manipulation leads to double free. An attack has to be approached locally. The identifier of the patch is 2f07ccdf21e705377862e5f9dfa31e1694979ac7. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2025-64524	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. In versions 2.0.1 and prior, a heap-buffer-overflow vulnerability in the rastertopclx filter causes the program to crash with a segmentation fault when processing maliciously crafted input data. This issue can be exploited to trigger memory corruption, potentially leading to arbitrary code execution. This issue has been patched via commit 956283c.	3.3	More Details
CVE-2025-65961	Contao is an Open Source CMS. From version 4.0.0 to before 4.13.57, before 5.3.42, and before 5.6.5, it is possible to inject code into the template output that will be executed in the browser in the front end and back end. This issue has been patched in versions 4.13.57, 5.3.42, and 5.6.5. A workaround for this issue involves not using the affected templates or patch them manually.	3.3	More Details
CVE-2025-33199	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker could cause incorrect control flow behavior. A successful exploit of this vulnerability might lead to data tampering.	3.2	More Details
CVE-2025-13643	A user with access to the cluster with a limited set of privilege actions may be able to terminate queries that are being executed by other users. This may cause a denial of service by preventing a fraction of queries from successfully completing. This issue affects MongoDB Server v7.0 versions prior to 7.0.26 and MongoDB Server v8.0 versions prior to 8.0.14	3.1	More Details
CVE-2025-65942	VictoriaMetrics is a scalable solution for monitoring and managing time series data. In versions from 1.0.0 to before 1.110.23, from 1.111.0 to before 1.122.8, and from 1.123.0 to before 1.129.1, affected versions are vulnerable to DoS attacks because the snappy decoder ignored VictoriaMetrics request size limits allowing malformed blocks to trigger excessive memory use. This could lead to OOM errors and service instability. The fix enforces block-size checks based on MaxRequest limits. This issue has been patched in versions 1.110.23, 1.122.8, and 1.129.1.	2.7	More Details
CVE-2025-13484	A vulnerability was identified in Campcodes Complete Online Beauty Parlor Management System 1.0. This vulnerability affects unknown code of the file /admin/customer-list.php. The manipulation of the argument Name leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	2.4	More Details
CVE-2025-13469	A security vulnerability has been detected in Public Knowledge Project omp and ojs 3.3.0/3.4.0/3.5.0. Impacted is an unknown function of the file plugins/paymethod/manual/templates/paymentForm.tpl of the component Payment Instructions Setting Handler. The manipulation of the argument manualInstructions leads to cross site scripting. The attack can be initiated remotely. You should upgrade the affected component.	2.4	More Details
CVE-2025-13412	A vulnerability was determined in Campcodes Retro Basketball Shoes Online Store 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_running.php. Executing manipulation of the argument product_name can lead to cross site scripting. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-2025-31216	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.7, iOS 18.5 and iPadOS 18.5. An attacker with physical access to a device may be able to override managed Wi-Fi profiles.	2.4	More Details
CVE-	NVIDIA DGX Spark GB10 contains a vulnerability in SROOT firmware, where an attacker		

2025-33200	could cause a resource to be reused. A successful exploit of this vulnerability might lead to information disclosure.	2.3	More Details
CVE-2025-62691	Security Point (Windows) of MaLion and MaLionCloud contains a stack-based buffer overflow vulnerability in processing HTTP headers. Receiving a specially crafted request from a remote unauthenticated attacker could lead to arbitrary code execution with SYSTEM privilege.	N/A	More Details
CVE-2025-51745	An issue was discovered in jishenghua JSH_ERP 2.3.1. The /role/addcan endpoint is vulnerable to fastjson deserialization attacks.	N/A	More Details
CVE-2025-59485	Incorrect default permissions issue exists in Security Point (Windows) of MaLion prior to Ver.5.3.4. If this vulnerability is exploited, an arbitrary file could be placed in the specific folder by a user who can log in to the system where the product's Windows client is installed. If the file is a specially crafted DLL file, arbitrary code could be executed with SYSTEM privilege.	N/A	More Details
CVE-2025-59372	A path traversal vulnerability has been identified in certain router models. A remote, authenticated attacker could exploit this vulnerability to write files outside the intended directory, potentially affecting device integrity. Refer to the 'Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-59371	An authentication bypass vulnerability has been identified in the IFTTT integration feature. A remote, authenticated attacker could leverage this vulnerability to potentially gain unauthorized access to the device. This vulnerability does not affect Wi-Fi 7 series models. Refer to the 'Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-66184	Rejected reason: Not used	N/A	More Details
CVE-2025-65944	Sentry-Javascript is an official Sentry SDKs for JavaScript. From version 10.11.0 to before 10.27.0, when a Node.js application using the Sentry SDK has sendDefaultPii: true it is possible to inadvertently send certain sensitive HTTP headers, including the Cookie header, to Sentry. Those headers would be stored within a Sentry organization as part of the associated trace. A person with access to the Sentry organization could then view and use these sensitive values to impersonate or escalate their privileges within the application. This issue has been patched in version 10.27.0.	N/A	More Details
CVE-2025-63735	A reflected Cross site scripting (XSS) vulnerability in Ruckus Unleashed 200.13.6.1.319 via the name parameter to the the captive-portal endpoint selfguestpass/guestAccessSubmit.jsp.	N/A	More Details
CVE-2025-51746	An issue was discovered in jishenghua JSH_ERP 2.3.1. The /serialNumber/addSerialNumber endpoint is vulnerable to fastjson deserialization attacks.	N/A	More Details
CVE-2025-64693	Security Point (Windows) of MaLion and MaLionCloud contains a heap-based buffer overflow vulnerability in processing Content-Length. Receiving a specially crafted request from a remote unauthenticated attacker could lead to arbitrary code execution with SYSTEM privilege.	N/A	More Details
CVE-2025-66183	Rejected reason: Not used	N/A	More Details
CVE-2025-66181	Rejected reason: Not used	N/A	More Details

CVE-2025-65952	Console is a network used to control Gorilla Tag mods' users and other users on the network. Prior to version 2.8.0, a path traversal vulnerability exists where complicated combinations of backslashes and periods can be used to escape the Gorilla Tag path and write to unwanted directories. This issue has been patched in version 2.8.0.	N/A	More Details
CVE-2025-59370	A command injection vulnerability has been identified in bwdpi. A remote, authenticated attacker could leverage this vulnerability to potentially execute arbitrary commands, leading to the device executing unintended instructions. Refer to the 'Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-59369	A SQL injection vulnerability has been identified in bwdpi. A remote, authenticated attacker could leverage this vulnerability to potentially execute arbitrary SQL queries, leading to unauthorized data access. Refer to the 'Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-59368	An integer underflow vulnerability has been identified in Aicloud. An authenticated attacker may trigger this vulnerability by sending a crafted request, potentially impacting the availability of the device. Refer to the ' Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-59366	An authentication-bypass vulnerability exists in AiCloud. This vulnerability can be triggered by an unintended side effect of the Samba functionality, potentially leading to allow execution of specific functions without proper authorization. Refer to the Security Update for ASUS Router Firmware section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-59365	A stack buffer overflow vulnerability has been identified in certain router models. An authenticated attacker may trigger this vulnerability by sending a crafted request, potentially impacting the availability of the device. Refer to the ' Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-66182	Rejected reason: Not used	N/A	More Details
CVE-2025-66185	Rejected reason: Not used	N/A	More Details
CVE-2025-51744	An issue was discovered in jishenghua JSH_ERP 2.3.1. The /user/addUser endpoint is vulnerable to fastjson deserialization attacks.	N/A	More Details
CVE-2025-66180	Rejected reason: Not used	N/A	More Details
CVE-2025-12742	A Looker user with a Developer role could cause Looker to execute a malicious command, due to insecure processing of Teradata driver parameters. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted instances. No user action is required for these. Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.12.108+ * 24.18.200+ * 25.0.78+ * 25.6.65+ * 25.8.47+ * 25.12.10+ * 25.14+	N/A	More Details
	OpenBao is an open source identity-based secrets management system. Prior to version 2.4.4, a privileged operator could use the identity group subsystem to add a root policy to a group identity group, escalating their or another user's permissions in		

CVE-2025-64761	the system. Specifically this is an issue when: an operator in the root namespace has access to identity/groups endpoints and an operator does not have policy access. Otherwise, an operator with policy access could create or modify an existing policy to grant root-equivalent permissions through the sudo capability. This issue has been patched in version 2.4.4.	N/A	More Details
CVE-2025-9803	lunary-ai/lunary version 1.9.34 is vulnerable to an account takeover due to improper authentication in the Google OAuth integration. The application fails to verify the 'aud' (audience) field in the access token issued by Google, which is crucial for ensuring the token is intended for the application. This oversight allows attackers to use tokens issued to malicious applications to gain unauthorized access to user accounts. The issue is resolved in version 1.9.35.	N/A	More Details
CVE-2025-59373	A local privilege escalation vulnerability exists in the restore mechanism of ASUS System Control Interface. It can be triggered when an unprivileged actor copies files without proper validation into protected system paths, potentially leading to arbitrary files being executed as SYSTEM. For more information, please refer to section Security Update for MyAsus in the ASUS Security Advisory.	N/A	More Details
CVE-2025-51742	An issue was discovered in jishenghua JSH_ERP 2.3.1. The /material/getMaterialEnableSerialNumberList endpoint passes the search query parameter directly to parseObject(), introducing a Fastjson deserialization vulnerability that can lead to RCE via JDBC payloads.	N/A	More Details
CVE-2025-34350	UnForm Server versions < 10.1.15 contain an unauthenticated arbitrary file read and SMB coercion vulnerability in the Doc Flow feature’s 'arc' endpoint. The Doc Flow module uses the 'arc' handler to retrieve and render pages or resources specified by the user-supplied 'pp' parameter, but it does so without enforcing authentication or restricting path inputs. As a result, an unauthenticated remote attacker can supply local filesystem paths to read arbitrary files accessible to the service account. On Windows deployments, providing a UNC path can also coerce the server into initiating outbound SMB authentication, potentially exposing NTLM credentials for offline cracking or relay. This issue may lead to sensitive information disclosure and, in some environments, enable further lateral movement.	N/A	More Details
CVE-2025-65085	A Heap-based Buffer Overflow vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions 12.6.1204.207 and prior that could allow an attacker to disclose information or execute arbitrary code.	N/A	More Details
CVE-2025-65084	An Out-of-Bounds Write vulnerability is present in Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, and Cobalt Share versions 12.6.1204.207 and prior that could allow an attacker to disclose information or execute arbitrary code.	N/A	More Details
CVE-2025-12003	A path traversal vulnerability has been identified in WebDAV, which may allow unauthenticated remote attackers to impact the integrity of the device. Refer to the ' Security Update for ASUS Router Firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-64062	The Primakon Pi Portal 1.0.18 /api/V2/pp_users?email endpoint is used for user data filtering but lacks proper server-side validation against the authenticated session. By manipulating the email parameter to an arbitrary value (e.g., otheruser@user.com), an attacker can assume the session and gain full access to the target user's data and privileges. Also, if the email parameter is left blank, the application defaults to the first user in the list, who is typically the application administrator, resulting in an immediate Privilege Escalation to the highest level.	N/A	More Details
CVE-2025-13483	SiRcom SMART Alert (SiSA) allows unauthorized access to backend APIs. This allows an unauthenticated attacker to bypass the login screen using browser developer tools, gaining access to restricted parts of the application.	N/A	More Details

CVE-2025-65965	Grype is a vulnerability scanner for container images and filesystems. A credential disclosure vulnerability was found in Grype, affecting versions 0.68.0 through 0.104.0. If registry credentials are defined and the output of grype is written using the --file or --output json=<file> option, the registry credentials will be included unsanitized in the output file. This issue has been patched in version 0.104.1. Users running affected versions of grype can work around this vulnerability by redirecting stdout to a file instead of using the --file or --output options.	N/A	More Details
CVE-2025-66186	Rejected reason: Not used	N/A	More Details
CVE-2025-64730	Cross-site scripting vulnerability exists in SNC-CX600W all versions. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the product.	N/A	More Details
CVE-2025-66179	Rejected reason: Not used	N/A	More Details
CVE-2025-66016	CGGMP24 is a state-of-art ECDSA TSS protocol that supports 1-round signing (requires 3 preprocessing rounds), identifiable abort, and a key refresh protocol. Prior to version 0.6.3, there is a missing check in the ZK proof that enables an attack in which single malicious signer can reconstruct full private key. This issue has been patched in version 0.6.3, for full mitigation it is recommended to upgrade to cggmp24 version 0.7.0-alpha.2 as it contains more security checks.	N/A	More Details
CVE-2025-66017	CGGMP24 is a state-of-art ECDSA TSS protocol that supports 1-round signing (requires 3 preprocessing rounds), identifiable abort, and a key refresh protocol. In versions 0.6.3 and prior of cggmp21 and version 0.7.0-alpha.1 of cggmp24, presignatures can be used in the way that significantly reduces security. cggmp24 version 0.7.0-alpha.2 release contains API changes that make it impossible to use presignatures in contexts in which it reduces security.	N/A	More Details
CVE-2025-9624	A vulnerability in OpenSearch allows attackers to cause Denial of Service (DoS) by submitting complex query_string inputs. This issue affects all OpenSearch versions below 3.2.0.	N/A	More Details
CVE-2025-64304	"FOD" App uses hard-coded cryptographic keys, which may allow a local unauthenticated attacker to retrieve the cryptographic keys.	N/A	More Details
CVE-2025-62497	Cross-site request forgery vulnerability exists in SNC-CX600W versions prior to Ver.2.8.0. If a user accesses a specially crafted webpage while logged in, unintended operations may be performed.	N/A	More Details
CVE-2025-51743	An issue was discovered in jishenghua JSH_ERP 2.3.1. The /materialCategory/addMaterialCategory endpoint is vulnerable to fastjson deserialization attacks.	N/A	More Details
CVE-2025-66187	Rejected reason: Not used	N/A	More Details
CVE-2025-64065	The Primakon Pi Portal 1.0.18 API /api/V2/pp_udfv_admin endpoint, fails to perform necessary server-side validation. The administrative LoginAs or user impersonation feature is vulnerable to a access control failure. This flaw allows any authenticated low-privileged user to execute a direct PATCH request, enabling them to impersonate any other arbitrary user, including application Administrators. This is due to a Broken Function Level Authorization failure (the function doesn't check the caller's privilege) compounded by an Insecure Design that permits a session switch without requiring the target user's password or an administrative token and only needs email of user.	N/A	More Details

CVE-2025-12852	DLL Loading vulnerability in NEC Corporation RakurakuMusen Start EX All Verisons allows a attacker to manipulate the PC environment to cause unintended operations on the user's device.	N/A	More Details
CVE-2025-66093	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hupe13 Extensions for Leaflet Map extensions-leaflet-map allows DOM-Based XSS.This issue affects Extensions for Leaflet Map: from n/a through <= 4.8.	N/A	More Details
CVE-2024-14007	Shenzhen TVT Digital Technology Co., Ltd. NVMS-9000 firmware (used by many white-labeled DVR/NVR/IPC products) versions prior to 1.3.4 contain an authentication bypass in the NVMS-9000 control protocol. By sending a single crafted TCP payload to an exposed NVMS-9000 control port, an unauthenticated remote attacker can invoke privileged administrative query commands without valid credentials. Successful exploitation discloses sensitive information including administrator usernames and passwords in cleartext, network and service configuration, and other device details via commands such as queryBasicCfg, queryUserList, queryEmailCfg, queryPPPoECfg, and queryFTPCfg.	N/A	More Details
CVE-2023-7330	Ruijie NBR series routers contain an unauthenticated arbitrary file upload vulnerability via /ddi/server/fileupload.php. The endpoint accepts attacker-supplied values in the name and uploadDir parameters and saves the provided multipart file content without adequate validation or sanitization of file type, path, or extension. A remote attacker can upload a crafted PHP file and then access it from the web root, resulting in arbitrary code execution in the context of the web service. Exploitation evidence was observed by the Shadowserver Foundation on 2025-01-14 UTC.	N/A	More Details
CVE-2025-13315	Twonky Server 8.5.2 on Linux and Windows is vulnerable to an access control flaw. An unauthenticated attacker can bypass web service API authentication controls to leak a log file and read the administrator's username and encrypted password.	N/A	More Details
CVE-2025-65095	Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other. Prior to version 1.35.1, there is potential cross-site scripting on index and tree page. This issue has been patched in version 1.35.1.	N/A	More Details
CVE-2025-65094	WBCE CMS is a content management system. Prior to version 1.6.4, a low-privileged user in WBCE CMS can escalate their privileges to the Administrators group by manipulating the groups[] parameter in the /admin/users/save.php request. The UI restricts users to assigning only their existing group, but server-side validation is missing, allowing attackers to overwrite their group membership and obtain full administrative access. This results in a complete compromise of the CMS. This issue has been patched in version 1.6.4.	N/A	More Details
CVE-2025-65100	Isar is an integration system for automated root filesystem generation. In versions 0.11-rc1 and 0.11, defining ISAR_APT_SNAPSHOT_DATE alone does not set the correct timestamp value for security distribution, leading to missed security updates. This issue has been patched via commit 738bcbb.	N/A	More Details
CVE-2025-11884	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in opentext uCMDB allows Stored XSS. The vulnerability could allow an attacker has high level access to UCMDB to create or update data with malicious scripts This issue affects uCMDB: 24.4.	N/A	More Details
CVE-2025-4042	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11676	Improper input validation vulnerability in TP-Link System Inc. TL-WR940N V6 (UPnP modules), which allows unauthenticated adjacent attackers to perform DoS attack. This issue affects TL-WR940N V6 <= Build 220801.	N/A	More Details

CVE-2025-12414	An attacker could take over a Looker account in a Looker instance configured with OIDC authentication, due to email address string normalization.Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted. Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.12.100+ * 24.18.193+ * 25.0.69+ * 25.6.57+ * 25.8.39+ * 25.10.22+ * 25.12.0+	N/A	More Details
CVE-2024-31405	Rejected reason: Voluntarily withdrawn	N/A	More Details
CVE-2025-13425	A bug in the filesystem traversal fallback path causes fs/diriterate/diriterate.go:Next() to overindex an empty slice when ReadDir returns nil for an empty directory, resulting in a panic (index out of range) and an application crash (denial of service) in OSV-SCALIBR.	N/A	More Details
CVE-2025-34320	BASIS BBj versions prior to 25.00 contain a Jetty-served web endpoint that fails to properly validate or canonicalize input path segments. This allows unauthenticated directory traversal sequences to cause the server to read arbitrary system files accessible to the account running the service. Retrieved configuration artifacts may contain account credentials used for BBj Enterprise Manager; possession of these credentials enables administrative access and use of legitimate management functionality that can result in execution of system commands under the service account. Depending on the operating system and the privileges of the BBj service account, this issue may also allow access to other sensitive files on the host, including operating system or application data, potentially exposing additional confidential information.	N/A	More Details
CVE-2025-62875	An Improper Check for Unusual or Exceptional Conditions vulnerability in OpenSMTPD allows local users to crash OpenSMTPD. This issue affects openSUSE Tumbleweed: from ? before 7.8.0p0-1.1.	N/A	More Details
CVE-2025-13437	When zx is invoked with --prefer-local=<path>, the CLI creates a symlink named ./node_modules pointing to <path>/node_modules. Due to a logic error in src/cli.ts (linkNodeModules / cleanup), the function returns the target path instead of the alias (symlink path). The later cleanup routine removes what it received, which deletes the target directory itself. Result: zx can delete an external <path>/node_modules outside the current working directory.	N/A	More Details
CVE-2025-64185	Open OnDemand is an open-source HPC portal. Prior to versions 4.0.8 and 3.1.16, Open OnDemand packages create world writable locations in the GEM_PATH. Open OnDemand versions 4.0.8 and 3.1.16 have been patched for this vulnerability.	N/A	More Details
CVE-2025-55126	HackerOne community member Dang Hung Vi (vidang04) has reported a stored XSS vulnerability involving the navigation box at the top of advertiser-related pages, with campaign names being the vector for the stored XSS	N/A	More Details
CVE-2025-55128	HackerOne community member Dao Hoang Anh (yoyomiski) has reported an uncontrolled resource consumption vulnerability in the “userlog-index.php”. An attacker with access to the admin interface could request an arbitrarily large number of items per page, potentially leading to a denial of service	N/A	More Details
CVE-2025-48986	Authorization bypass in Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes an logged in attacker to change other users' email address and potentialy take over their accounts using the forgot password functionality.	N/A	More Details
CVE-2025-52666	Improper neutralisation of format characters in the settings of Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes an administrator user to disable the admin user console due to a fatal PHP error.	N/A	More Details

CVE-2025-52667	Missing JSON Content-Type header in a script in Revive Adserver 6.0.1 and 5.5.2 and earlier versions causes a stored XSS attack to be possible for a logged in manager user.	N/A	More Details
CVE-2025-52668	Improper input neutralization in the stats-conversions.php script in Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes potential information disclosure and session hijacking via a stored XSS attack.	N/A	More Details
CVE-2025-52669	Insecure design policies in the user management system of Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes non-admin users to have access to the contact name and email address of other users on the system.	N/A	More Details
CVE-2025-52670	Missing authorization check in Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes users on the system to delete banners owned by other accounts	N/A	More Details
CVE-2025-52671	Debug information disclosure in the SQL error message to in Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes non-admin users to acquire information about the software, PHP and database versions currently in use.	N/A	More Details
CVE-2025-55123	Improper neutralization of input in Revive Adserver 5.5.2 and 6.0.1 and earlier versions causes manager accounts to be able to craft XSS attacks to their own advertiser users.	N/A	More Details
CVE-2025-55124	Improper neutralisation of input in Revive Adserver 6.0.0+ causes a reflected XSS attack in the banner-zone.php script.	N/A	More Details
CVE-2025-62372	vLLM is an inference and serving engine for large language models (LLMs). From version 0.5.5 to before 0.11.1, users can crash the vLLM engine serving multimodal models by passing multimodal embedding inputs with correct ndim but incorrect shape (e.g. hidden dimension is wrong), regardless of whether the model is intended to support such inputs (as defined in the Supported Models page). This issue has been patched in version 0.11.1.	N/A	More Details
CVE-2025-64751	OpenFGA is a high-performance and flexible authorization/permission engine built for developers and inspired by Google Zanzibar. OpenFGA v1.4.0 to v1.11.0 (openfga-0.1.34 <= Helm chart <= openfga-0.2.48, v.1.4.0 <= docker <= v.1.11.0) are vulnerable to improper policy enforcement when certain Check and ListObject calls are executed. This issue has been patched in version 1.11.1.	N/A	More Details
CVE-2025-64755	Claude Code is an agentic coding tool. Prior to version 2.0.31, due to an error in sed command parsing, it was possible to bypass the Claude Code read-only validation and write to arbitrary files on the host system. This issue has been patched in version 2.0.31.	N/A	More Details
CVE-2025-64762	The AuthKit library for Next.js provides convenient helpers for authentication and session management using WorkOS & AuthKit with Next.js. In authkit-nextjs version 2.11.0 and below, authenticated responses do not defensively apply anti-caching headers. In environments where CDN caching is enabled, this can result in session tokens being included in cached responses and subsequently served to multiple users. Next.js applications deployed on Vercel are unaffected unless they manually enable CDN caching by setting cache headers on authenticated paths. Patched in authkit-nextjs 2.11.1, which applies anti-caching headers to all responses behind authentication.	N/A	More Details
	eGovFramework/egovframe-common-components versions up to and including 4.3.1 includes Web Editor image upload and related file delivery functionality that uses symmetric encryption to protect URL parameters, but exposes an encryption oracle that allows attackers to generate valid ciphertext for chosen values. The image upload endpoints /utl/wed/insertImage.do and /utl/wed/insertImageCk.do encrypt server-side		

CVE-2025-34337	paths, filenames, and MIME types and embed them directly into a download URL that is returned to the client. Because these same encrypted parameters are trusted by other endpoints, such as /utl/web/imageSrc.do and /cmm/fms/getImage.do, an unauthenticated attacker can abuse the upload functionality to obtain encrypted representations of attacker-chosen identifiers and then replay those ciphertext values to file-serving APIs. This design failure allows an attacker to bypass access controls that rely solely on the secrecy of encrypted parameters and retrieve arbitrary stored files that are otherwise expected to require an existing session or specific authorization context. KISA/KrCERT has identified this unpatched vulnerability as "KVE-2023-5281."	N/A	More Details
CVE-2025-34336	eGovFramework/egovframe-common-components versions up to and including 4.3.1 contain an unauthenticated file upload vulnerability via the /utl/wed/insertImage.do and /utl/wed/insertImageCk.do image upload endpoints. These controllers accept multipart requests without authentication, pass the uploaded content to a shared upload helper, and store the file on the server under a framework-controlled path. The framework then returns a download URL that can be used to retrieve the uploaded content, including an attacker-controlled Content-Type within the limits of the image upload functionality. While a filename extension whitelist is enforced, the attacker fully controls the file contents. The response MIME type used is also attacker-controlled when the file is served up to version < 4.1.2. Since version 4.1.2, it is possible to download any image uploaded with any whitelisted content type. But any file uploaded other than an image will be served with the `application/octet-stream` content type (the content type is no longer controlled by the attacker since version 4.1.2). This enables an unauthenticated attacker to use any affected application as a persistent file hosting service for arbitrary content under the application's origin. KISA/KrCERT has identified this unpatched vulnerability as "KVE-2023-5280."	N/A	More Details
CVE-2025-34335	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 expose an authenticated command injection vulnerability in the license activation workflow handled by AudioCodes_files/ActivateLicense.php. When a license file is uploaded, the application derives a new filename by combining a generated base name with the attacker-controlled extension portion of the original upload name, then constructs a command line for fax_server_lic_cmdline.exe that includes this path. The extension value is incorporated into the command string without input validation, escaping, or proper argument quotation before being passed to exec(). An authenticated user with access to the license upload interface can supply a specially crafted filename whose extension injects additional shell metacharacters, causing arbitrary commands to be executed as NT AUTHORITY\\SYSTEM.	N/A	More Details
CVE-2025-0351	Rejected reason: Voluntarily withdrawn	N/A	More Details
CVE-2025-13051	When the service of ABP and AES is installed in a directory writable by non-administrative users, an attacker can replace or plant a DLL with the same name as one loaded by the service. Upon service restart, the malicious DLL is loaded and executed under the LocalSystem account, resulting in unauthorized code execution with elevated privileges. This issue affects ABP and AES: from ABP 2.0 through 2.0.7.9050, from AES 1.0 through 1.0.6.8290.	N/A	More Details
CVE-2025-65933	Rejected reason: Not used	N/A	More Details
CVE-2025-65934	Rejected reason: Not used	N/A	More Details
CVE-2025-	Rejected reason: Not used	N/A	More Details

65935			
CVE-2025-65936	Rejected reason: Not used	N/A	More Details
CVE-2025-65937	Rejected reason: Not used	N/A	More Details
CVE-2025-65938	Rejected reason: Not used	N/A	More Details
CVE-2025-65939	Rejected reason: Not used	N/A	More Details
CVE-2025-65940	Rejected reason: Not used	N/A	More Details
CVE-2025-65941	Rejected reason: Not used	N/A	More Details
CVE-2025-11243	Allocation of Resources Without Limits or Throttling vulnerability in Shelly Pro 4PM (before v1.6) allows Excessive Allocation via network.	N/A	More Details
CVE-2025-12056	Out-of-bounds Read in Shelly Pro 3EM (before v1.4.4) allows Overread Buffers.	N/A	More Details
CVE-2025-11446	Insertion of Sensitive Information into Log File vulnerability in upKeeper Solutions upKeeper Manager allows Use of Known Domain Credentials.This issue affects upKeeper Manager: from 5.2.0 before 5.2.12.	N/A	More Details
CVE-2025-12472	An attacker with a Looker Developer role could manipulate a LookML project to exploit a race condition during Git directory deletion, leading to arbitrary command execution on the Looker instance. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted instances. No user action is required for these. Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.12.103+ * 24.18.195+ * 25.0.72+ * 25.6.60+ * 25.8.42+ * 25.10.22+	N/A	More Details
CVE-2025-34334	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 are vulnerable to an authenticated command injection in the fax test functionality implemented by AudioCodes_files/TestFax.php. When a fax "send" test is requested, the application builds a faxsender command line using attacker-supplied parameters and passes it to GlobalUtils::RunBatchFile without proper validation or shell-argument sanitization. The resulting batch file is written into a temporary run directory and then executed via a backend service that runs as NT AUTHORITY\\SYSTEM. An authenticated attacker with access to the fax test interface can craft parameter values that inject additional shell commands into the generated batch file, leading to arbitrary command execution with SYSTEM privileges. In addition, because the generated batch files reside in a location with overly permissive file system permissions, a local low-privilege user on the server can modify pending batch files to achieve the same elevation.	N/A	More Details

CVE-2025-12592	Legacy Vivotek Device firmware uses default credetials for the root and user login accounts.	N/A	More Details
CVE-2024-8527	Open Redirect in URL parameter in Automated Logic WebCTRL and Carrier i-Vu versions 6.0, 6.5, 7.0, 8.0, 8.5, 9.0 may allow attackers to exploit user sessions.	N/A	More Details
CVE-2024-8528	Reflected XSS using a specific URL in Automated Logic WebCTRL and Carrier i-VU can allow delivery of malicious payload due to a specific GET parameter not being sanitized.	N/A	More Details
CVE-2025-10702	Improper Control of Generation of Code ('Code Injection') vulnerability in Progress DataDirect Connect for JDBC drivers, Progress DataDirect Open Access JDBC driver and Hybrid Data Pipeline allows Remote Code Inclusion. The SpyAttribute connection option implemented by the DataDirect Connect for JDBC drivers, DataDirect Hybrid Data Pipeline JDBC driver and the DataDirect OpenAccess JDBC driver supports an undocumented syntax construct for the option value that if discovered can be used by an attacker. If an application allows an end user to specify a value for the SpyAttributes connection option then an attacker can use the undocumented syntax to cause the driver to load an arbitrary class on the class path and execute a constructor on that class. This issue affects: DataDirect Connect for JDBC for Amazon Redshift: through 6.0.0.001392, fixed in 6.0.0.001541 DataDirect Connect for JDBC for Apache Cassandra: through 6.0.0.000805, fixed in 6.0.0.000833 DataDirect Connect for JDBC for Hive: through 6.0.1.001499, fixed in 6.0.1.001628 DataDirect Connect for JDBC for Apache Impala: through 6.0.0.001155, fixed in 6.0.0.001279 DataDirect Connect for JDBC for Apache SparkSQL: through 6.0.1.001222, fixed in 6.0.1.001344 DataDirect Connect for JDBC Autonomous REST Connector: through 6.0.1.006961, fixed in 6.0.1.007063 DataDirect Connect for JDBC for DB2: through 6.0.0.000717, fixed in 6.0.0.000964 DataDirect Connect for JDBC for Google Analytics 4: through 6.0.0.000454, fixed in 6.0.0.000525 DataDirect Connect for JDBC for Google BigQuery: through 6.0.0.002279, fixed in 6.0.0.002410 DataDirect Connect for JDBC for Greenplum: through 6.0.0.001712, fixed in 6.0.0.001727 DataDirect Connect for JDBC for Informix: through 6.0.0.000690, fixed in 6.0.0.0851 DataDirect Connect for JDBC for Microsoft Dynamics 365: through 6.0.0.003161, fixed in 6.0.0.3198 DataDirect Connect for JDBC for Microsoft SQLServer: through 6.0.0.001936, fixed in 6.0.0.001957 DataDirect Connect for JDBC for Microsoft Sharepoint: through 6.0.0.001559, fixed in 6.0.0.001587 DataDirect Connect for JDBC for MongoDB: through 6.1.0.001654, fixed in 6.1.0.001669 DataDirect Connect for JDBC for MySQL: through 5.1.4.000330, fixed in 5.1.4.000364 DataDirect Connect for JDBC for Oracle Database: through 6.0.0.001747, fixed in 6.0.0.001776 DataDirect Connect for JDBC for Oracle Eloqua: through 6.0.0.001438, fixed in 6.0.0.001458 DataDirect Connect for JDBC for Oracle Sales Cloud: through 6.0.0.001225, fixed in 6.0.0.001316 DataDirect Connect for JDBC for Oracle Service Cloud: through 5.1.4.000298, fixed in 5.1.4.000309 DataDirect Connect for JDBC for PostgreSQL: through 6.0.0.001843, fixed in 6.0.0.001856 DataDirect Connect for JDBC for Progress OpenEdge: through 5.1.4.000187, fixed in 5.1.4.000189 DataDirect Connect for JDBC for Salesforce: through 6.0.0.003020, fixed in 6.0.0.003125 DataDirect Connect for JDBC for SAP HANA: through 6.0.0.000879, product retired DataDirect Connect for JDBC for SAP S/4 HANA: through 6.0.1.001818, fixed in 6.0.1.001858 DataDirect Connect for JDBC for Sybase ASE: through 5.1.4.000161, fixed in 5.1.4.000162 DataDirect Connect for JDBC for Snowflake: through 6.0.1.001821, fixed in 6.0.1.001856 DataDirect Hybrid Data Pipeline Server: through 4.6.2.3309, fixed in 4.6.2.3430 DataDirect Hybrid Data Pipeline JDBC Driver: through 4.6.2.0607, fixed in 4.6.2.1023 DataDirect Hybrid Data Pipeline On Premises Connector: through 4.6.2.1223, fixed in 4.6.2.1339 DataDirect Hybrid Data Pipeline Docker: through 4.6.2.3316, fixed in 4.6.2.3430 DataDirect OpenAccess JDBC Driver: through 8.1.0.0177, fixed in 8.1.0.0183 DataDirect OpenAccess JDBC Driver: through 9.0.0.0019, fixed in 9.0.0.0022	N/A	More Details
	Improper Control of Generation of Code ('Code Injection') vulnerability in Progress		

CVE-2025-10703	DataDirect Connect for JDBC drivers, Progress DataDirect Open Access JDBC driver and Hybrid Data Pipeline allows Remote Code Inclusion. The SpyAttribute connection option implemented by the DataDirect Connect for JDBC drivers, DataDirect Hybrid Data Pipeline JDBC driver and the DataDirect OpenAccess JDBC driver log=(file) construct allows the user to specify an arbitrary file for the JDBC driver to write its log information to. If an application allows an end user to specify a value for the SpyAttributes connection option then an attacker could cause java script to be written to a log file. If the log file was in the correct location with the correct extension, an application server could see that log file as a resource to be served. The attacker could fetch the resource from the server causing the java script to be executed. This issue affects: DataDirect Connect for JDBC for Amazon Redshift: through 6.0.0.001392, fixed in 6.0.0.001541 DataDirect Connect for JDBC for Apache Cassandra: through 6.0.0.000805, fixed in 6.0.0.000833 DataDirect Connect for JDBC for Hive: through 6.0.1.001499, fixed in 6.0.1.001628 DataDirect Connect for JDBC for Apache Impala: through 6.0.0.001155, fixed in 6.0.0.001279 DataDirect Connect for JDBC for Apache SparkSQL: through 6.0.1.001222, fixed in 6.0.1.001344 DataDirect Connect for JDBC Autonomous REST Connector: through 6.0.1.006961, fixed in 6.0.1.007063 DataDirect Connect for JDBC for DB2: through 6.0.0.000717, fixed in 6.0.0.000964 DataDirect Connect for JDBC for Google Analytics 4: through 6.0.0.000454, fixed in 6.0.0.000525 DataDirect Connect for JDBC for Google BigQuery: through 6.0.0.002279, fixed in 6.0.0.002410 DataDirect Connect for JDBC for Greenplum: through 6.0.0.001712, fixed in 6.0.0.001727 DataDirect Connect for JDBC for Informix: through 6.0.0.000690, fixed in 6.0.0.0851 DataDirect Connect for JDBC for Microsoft Dynamics 365: through 6.0.0.003161, fixed in 6.0.0.3198 DataDirect Connect for JDBC for Microsoft SQLServer: through 6.0.0.001936, fixed in 6.0.0.001957 DataDirect Connect for JDBC for Microsoft Sharepoint: through 6.0.0.001559, fixed in 6.0.0.001587 DataDirect Connect for JDBC for MongoDB: through 6.1.0.001654, fixed in 6.1.0.001669 DataDirect Connect for JDBC for MySQL: through 5.1.4.000330, fixed in 5.1.4.000364 DataDirect Connect for JDBC for Oracle Database: through 6.0.0.001747, fixed in 6.0.0.001776 DataDirect Connect for JDBC for Oracle Eloqua: through 6.0.0.001438, fixed in 6.0.0.001458 DataDirect Connect for JDBC for Oracle Sales Cloud: through 6.0.0.001225, fixed in 6.0.0.001316 DataDirect Connect for JDBC for Oracle Service Cloud: through 5.1.4.000298, fixed in 5.1.4.000309 DataDirect Connect for JDBC for PostgreSQL: through 6.0.0.001843, fixed in 6.0.0.001856 DataDirect Connect for JDBC for Progress OpenEdge: through 5.1.4.000187, fixed in 5.1.4.000189 DataDirect Connect for JDBC for Salesforce: through 6.0.0.003020, fixed in 6.0.0.003125 DataDirect Connect for JDBC for SAP HANA: through 6.0.0.000879, product retired DataDirect Connect for JDBC for SAP S/4 HANA: through 6.0.1.001818, fixed in 6.0.1.001858 DataDirect Connect for JDBC for Sybase ASE: through 5.1.4.000161, fixed in 5.1.4.000162 DataDirect Connect for JDBC for Snowflake: through 6.0.1.001821, fixed in 6.0.1.001856 DataDirect Hybrid Data Pipeline Server: through 4.6.2.3309, fixed in 4.6.2.3430 DataDirect Hybrid Data Pipeline JDBC Driver: through 4.6.2.0607, fixed in 4.6.2.1023 DataDirect Hybrid Data Pipeline On Premises Connector: through 4.6.2.1223, fixed in 4.6.2.1339 DataDirect Hybrid Data Pipeline Docker: through 4.6.2.3316, fixed in 4.6.2.3430 DataDirect OpenAccess JDBC Driver: through 8.1.0.0177, fixed in 8.1.0.0183 DataDirect OpenAccess JDBC Driver: through 9.0.0.0019, fixed in 9.0.0.0022	N/A	More Details
CVE-2025-63221	The Axel Technology puma devices (firmware versions 0.8.5 to 1.0.3) are vulnerable to Broken Access Control due to missing authentication on the /cgi-bin/gstFcgi.fcgi endpoint. Unauthenticated remote attackers can list user accounts, create new administrative users, delete users, and modify system settings, leading to full compromise of the device.	N/A	More Details
CVE-2025-	The Looker endpoint for generating new projects from database connections allows users to specify "looker" as a connection name, which is a reserved internal name for Looker's internal MySQL database. The schemas parameter is vulnerable to SQL injection, enabling attackers to manipulate SELECT queries that are constructed and executed against the internal MySQL database. This vulnerability allows users with developer permissions to extract data from Looker's internal MySQL database. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been	N/A	More

12743	mitigated for Looker-hosted instances. No user action is required for these. Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect against this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.12.106 * 24.18.198+ * 25.0.75 * 25.6.63+ * 25.8.45+ * 25.10.33+ * 25.12.1+ * 25.14+		Details
CVE-2025-34328	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 include a web administration component (F2MAdmin) that exposes an unauthenticated script-management endpoint at AudioCodes_files/utils/IVR/diagram/ajaxScript.php. The saveScript action writes attacker-supplied data directly to a server-side file path under the privileges of the web service account, which runs as NT AUTHORITY\\SYSTEM on Windows deployments. A remote, unauthenticated attacker can write arbitrary files into the product's web-accessible directory structure and subsequently execute them.	N/A	More Details
CVE-2025-34329	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 expose an unauthenticated backup upload endpoint at AudioCodes_files/ajaxBackupUploadFile.php in the F2MAdmin web interface. The script derives a backup folder path from application configuration, creates the directory if it does not exist, and then moves an uploaded file to that location using the attacker-controlled filename, without any authentication, authorization, or file-type validation. On default Windows deployments where the backup directory resolves to the system drive, a remote attacker can upload web server or interpreter configuration files that cause a log file or other server-controlled resource to be treated as executable code. This allows subsequent HTTP requests to trigger arbitrary command execution under the web server account, which runs as NT AUTHORITY\\SYSTEM.	N/A	More Details
CVE-2025-34330	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 include a web administration component (F2MAdmin) that exposes an unauthenticated prompt upload endpoint at AudioCodes_files/utils/IVR/diagram/ajaxPromptUploadFile.php. The script accepts an uploaded file and writes it into the C:\\F2MAdmin\\tmp directory using a filename derived from application constants, without any authentication, authorization, or file-type validation. A remote, unauthenticated attacker can upload or overwrite prompt- or music-on-hold–related files in this directory, potentially leading to tampering with IVR audio content or preparing files for use in further attacks.	N/A	More Details
CVE-2025-34331	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 contain an unauthenticated file read vulnerability via the download.php script. The endpoint exposes a file download mechanism that lacks access control, allowing remote, unauthenticated users to request files stored on the appliance based solely on attacker-supplied path and filename parameters. While limited to specific file extensions permitted by the application logic, sensitive backup archives can be retrieved, exposing internal databases and credential hashes. Successful exploitation may lead to disclosure of administrative password hashes and other sensitive configuration data.	N/A	More Details
CVE-2025-34332	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 include a web administration component that controls back-end Windows services using helper batch scripts located under C:\\F2MAdmin\\F2E\\AudioCodes_files\\utils\\Services. When certain service actions are requested through ajaxPost.php, these scripts are invoked by PHP using system() under the NT AUTHORITY\\SYSTEM account. The batch files in this directory are writable by any authenticated local user due to overly permissive ACLs, allowing them to replace script contents with arbitrary commands. On the next service start/stop operation, the modified script is executed as SYSTEM, enabling elevation of local privileges.	N/A	More Details
	AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including		

CVE-2025-34333	2.6.23 configure the web document root at C:\\F2MAdmin\\F2E with overly permissive file system permissions. Authenticated local users have modify rights on this directory, while the associated web server process runs as NT AUTHORITY\\SYSTEM. As a result, any local user can create or alter server-side scripts within the webroot and then trigger them via HTTP requests, causing arbitrary code to execute with SYSTEM privileges.	N/A	More Details
CVE-2025-58097	The installation directory of LogStare Collector is configured with incorrect access permissions. A non-administrative user may manipulate files within the installation directory and execute arbitrary code with the administrative privilege.	N/A	More Details
CVE-2025-61949	LogStare Collector contains a stored cross-site scripting vulnerability in UserManagement. If crafted user information is stored, an arbitrary script may be executed on the web browser of the user who logs in to the product's management page.	N/A	More Details
CVE-2025-62189	LogStare Collector contains an incorrect authorization vulnerability in UserRegistration. If exploited, a non-administrative user may create a new user account by sending a crafted HTTP request.	N/A	More Details
CVE-2025-12739	An attacker with viewer permissions in Looker could craft a malicious URL that, when opened by a Looker admin, would execute an attacker-supplied script. Exploitation required at least one Looker extension installed on the instance. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted instances. No user action is required for these. Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.18.201+ * 25.0.79+ * 25.6.66+ * 25.12.7+ * 25.16.0+ * 25.18.0+ * 25.20.0+	N/A	More Details
CVE-2025-11936	Improper input validation in the TLS 1.3 KeyShareEntry parsing in wolfSSL v5.8.2 on multiple platforms allows a remote unauthenticated attacker to cause a denial-of-service by sending a crafted ClientHello message containing duplicate KeyShareEntry values for the same supported group, leading to excessive CPU and memory consumption during ClientHello processing.	N/A	More Details
CVE-2025-12678	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-12888	Vulnerability in X25519 constant-time cryptographic implementations due to timing side channels introduced by compiler optimizations and CPU architecture limitations, specifically with the Xtensa-based ESP32 chips. If targeting Xtensa it is recommended to use the low memory implementations of X25519, which is now turned on as the default for Xtensa.	N/A	More Details
CVE-2025-65947	thread-amount is a tool that gets the amount of threads in the current process. Prior to version 0.2.2, there are resource leaks when querying thread counts on Windows and Apple platforms. In Windows platforms, the thread_amount function calls CreateToolhelp32Snapshot but fails to close the returned HANDLE using CloseHandle. Repeated calls to this function will cause the handle count of the process to grow indefinitely, eventually leading to system instability or process termination when the handle limit is reached. In Apple platforms, the thread_amount function calls task_threads (via Mach kernel APIs) which allocates memory for the thread list. The function fails to deallocate this memory using vm_deallocate. Repeated calls will result in a steady memory leak, eventually causing the process to be killed by the OOM (Out of Memory) killer. This issue has been patched in version 0.2.2.	N/A	More Details
CVE-2025-	With TLS 1.2 connections a client can use any digest, specifically a weaker digest that	N/A	More

12889	is supported, rather than those in the CertificateRequest.		Details
CVE-2025-12541	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-12561	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-13197	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-48507	The security state of the calling processor into Arm® Trusted Firmware (TF-A) is not used and could potentially allow non-secure processors access to secure memories, access to crypto operations, and the ability to turn on and off subsystems within the SOC.	N/A	More Details
CVE-2025-54515	The Secure Flag passed to Versal™ Adaptive SoC's Arm® Trusted Firmware for Cortex®-A processors (TF-A) for Arm's Power State Coordination Interface (PSCI) commands were incorrectly set to secure instead of using the processor's actual security state. This would allow the PSCI requests to appear they were from processors in the secure state instead of the non-secure state.	N/A	More Details
CVE-2025-12759	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-13589	FMS developed by Otsuka Information Technology has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	N/A	More Details
CVE-2025-13596	A sensitive information disclosure vulnerability exists in the error handling component of ATISoluciones CIGES Application version 2.15.6 and earlier. When certain unexpected conditions trigger unhandled exceptions, the application returns detailed error messages and stack traces to the client. This may expose internal filesystem paths, SQL queries, database connection details, or environment configuration data to remote unauthenticated attackers. This issue allows information gathering and reconnaissance but does not enable direct system compromise.	N/A	More Details
CVE-2025-12740	A Looker user with a Developer role could create a database connection using IBM DB2 driver and, by manipulating LookML, cause Looker to execute a malicious command, due to inadequate filtering of the driver's parameters. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted instances. No user action is required for these. Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 25.0.93+ * 25.6.84+ * 25.12.42+ * 25.14.50+ * 25.16.44+	N/A	More Details
CVE-2025-11933	Improper Input Validation in the TLS 1.3 CKS extension parsing in wolfSSL 5.8.2 and earlier on multiple platforms allows a remote unauthenticated attacker to potentially cause a denial-of-service via a crafted ClientHello message with duplicate CKS extensions.	N/A	More Details
CVE-	A Looker user with Developer role could create a database connection using Denodo driver and, by manipulating LookML, cause Looker to execute a malicious command. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted instances. No user action is required for these. Self-		

2025-12741	hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.12.108+ * 24.18.200+ * 25.0.78+ * 25.6.65+ * 25.8.47+ * 25.12.10+ * 25.14+	N/A	More Details
CVE-2025-41087	Cross-Site Scripting (XSS) vulnerability stored in tha Taclia web application, where the uploaded SVG images are not properly sanitized. This allows to the attackers to embed malicious scripts in SVG files such as image profiles, which are then stored on the server and executed in the context of any user who accesses the compromised resource.	N/A	More Details
CVE-2025-40212	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix refcount leak in nfsd_set_fh_dentry() nfsd exports a "pseudo root filesystem" which is used by NFSv4 to find the various exported filesystems using LOOKUP requests from a known root filehandle. NFSv3 uses the MOUNT protocol to find those exported filesystems and so is not given access to the pseudo root filesystem. If a v3 (or v2) client uses a filehandle from that filesystem, nfsd_set_fh_dentry() will report an error, but still stores the export in "struct svc_fh" even though it also drops the reference (exp_put()). This means that when fh_put() is called an extra reference will be dropped which can lead to use-after-free and possible denial of service. Normal NFS usage will not provide a pseudo-root filehandle to a v3 client. This bug can only be triggered by the client synthesising an incorrect filehandle. To fix this we move the assignments to the svc_fh later, after all possible error cases have been detected.	N/A	More Details
CVE-2025-41016	Inadequate access control vulnerability in Davantis DFUSION v6.177.7, which allows unauthorised actors to extract images and videos related to alarm events through access to “/alarms/<ALARM_ID>/<MEDIA>”, where the “MEDIA” parameter can take the value of “snapshot” or “video.mp4”. These media files contain images recorded by security cameras in response to triggered alerts.	N/A	More Details
CVE-2025-41017	Inadequate access control vulnerability in Davantis DDFUSION v6.177.7, which allows unauthorised actors to retrieve perspective parameters from security camera settings by accessing “/cameras/<CAMERA_ID>/perspective”.	N/A	More Details
CVE-2025-11921	iStats contains an insecure XPC service that allows local, unprivileged users to escalate their privileges to root via command injection.This issue affects iStats: 7.10.4.	N/A	More Details
CVE-2025-13541	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-13598	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-40213	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: fix crash in set_mesh_sync and set_mesh_complete There is a BUG: KASAN: stack-out-of-bounds in set_mesh_sync due to memcpy from badly declared on-stack flexible array. Another crash is in set_mesh_complete() due to double list_del via mgmt_pending_valid + mgmt_pending_remove. Use DEFINE_FLEX to declare the flexible array right, and don't memcpy outside bounds. As mgmt_pending_valid removes the cmd from list, use mgmt_pending_free, and also report status on error.	N/A	More Details
CVE-2025-13511	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This		More

2025-13594	candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	Details
CVE-2025-13466	body-parser 2.2.0 is vulnerable to denial of service due to inefficient handling of URL-encoded bodies with very large numbers of parameters. An attacker can send payloads containing thousands of parameters within the default 100KB request size limit, causing elevated CPU and memory usage. This can lead to service slowdown or partial outages under sustained malicious traffic. This issue is addressed in version 2.2.1.	N/A	More Details
CVE-2018-25126	Shenzhen TVT Digital Technology Co., Ltd. NVMS-9000 firmware (used by many white-labeled DVR/NVR/IPC products) contains hardcoded API credentials and an OS command injection flaw in its configuration services. The web/API interface accepts HTTP/XML requests authenticated with a fixed vendor credential string and passes user-controlled fields into shell execution contexts without proper argument sanitization. An unauthenticated remote attacker can leverage the hard-coded credential to access endpoints such as /editBlackAndWhiteList and inject shell metacharacters inside XML parameters, resulting in arbitrary command execution as root. The same vulnerable backend is also reachable in some models through a proprietary TCP service on port 4567 that accepts a magic GUID preface and base64-encoded XML, enabling the same command injection sink. Firmware releases from mid-February 2018 and later are reported to have addressed this issue. Exploitation evidence was observed by the Shadowserver Foundation on 2025-01-28 UTC.	N/A	More Details
CVE-2025-11934	Improper input validation in the TLS 1.3 CertificateVerify signature algorithm negotiation in wolfSSL 5.8.2 and earlier on multiple platforms allows for downgrading the signature algorithm used. For example when a client sends ECDSA P521 as the supported signature algorithm the server previously could respond as ECDSA P256 being the accepted signature algorithm and the connection would continue with using ECDSA P256, if the client supports ECDSA P256.	N/A	More Details
CVE-2025-11932	The server previously verified the TLS 1.3 PSK binder using a non-constant time method which could potentially leak information about the PSK binder	N/A	More Details
CVE-2025-62687	Cross-site request forgery vulnerability exists in LogStare Collector. If a user views a crafted page while logged, unintended operations may be performed.	N/A	More Details
CVE-2025-66111	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nelio Software Nelio Popups nelio-popups allows Stored XSS.This issue affects Nelio Popups: from n/a through <= 1.3.0.	N/A	More Details
CVE-2025-64299	LogStare Collector improperly handles the password hash data. An administrative user may obtain the other users' password hashes.	N/A	More Details
CVE-2025-64695	Uncontrolled search path element issue exists in the installer of LogStare Collector (for Windows). If exploited, arbitrary code may be executed with the privilege of the user invoking the installer.	N/A	More Details
CVE-2025-40209	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix memory leak of qgroup_list in btrfs_add_qgroup_relation When btrfs_add_qgroup_relation() is called with invalid qgroup levels (src >= dst), the function returns -EINVAL directly without freeing the preallocated qgroup_list structure passed by the caller. This causes a memory leak because the caller unconditionally sets the pointer to NULL after the call, preventing any cleanup. The issue occurs because the level validation check happens before the mutex is acquired and before any error handling path that would free the prealloc pointer. On this early return, the cleanup code at the 'out' label (which includes kfree(prealloc)) is never reached. In btrfs_ioctl_qgroup_assign(), the code pattern is: prealloc = kzalloc(sizeof(*prealloc), GFP_KERNEL); ret = btrfs_add_qgroup_relation(trans, sa->src, sa->dst, prealloc); prealloc = NULL; // Always	N/A	More Details

	set to NULL regardless of return value ... kfree(prealloc); // This becomes kfree(NULL), does nothing When the level check fails, 'prealloc' is never freed by either the callee or the caller, resulting in a 64-byte memory leak per failed operation. This can be triggered repeatedly by an unprivileged user with access to a writable btrfs mount, potentially exhausting kernel memory. Fix this by freeing prealloc before the early return, ensuring prealloc is always freed on all error paths.		
CVE-2025-40210	In the Linux kernel, the following vulnerability has been resolved: Revert "NFSD: Remove the cap on number of operations per NFSv4 COMPOUND" I've found that pynfs COMP6 now leaves the connection or lease in a strange state, which causes CLOSE9 to hang indefinitely. I've dug into it a little, but I haven't been able to root-cause it yet. However, I bisected to commit 48aab1606fa8 ("NFSD: Remove the cap on number of operations per NFSv4 COMPOUND"). Tianshuo Han also reports a potential vulnerability when decoding an NFSv4 COMPOUND. An attacker can place an arbitrarily large op count in the COMPOUND header, which results in: [51.410584] nfsd: vmalloc error: size 1209533382144, exceeds total pages, mode:0xdc0(GFP_KERNEL|__GFP_ZERO), nodemask=(null),cpuset=/,mems_allowed=0 when NFSD attempts to allocate the COMPOUND op array. Let's restore the operation-per-COMPOUND limit, but increased to 200 for now.	N/A	More Details
CVE-2025-40211	In the Linux kernel, the following vulnerability has been resolved: ACPI: video: Fix use-after-free in acpi_video_switch_brightness() The switch_brightness_work delayed work accesses device->brightness and device->backlight, freed by acpi_video_dev_unregister_backlight() during device removal. If the work executes after acpi_video_bus_unregister_backlight() frees these resources, it causes a use-after-free when acpi_video_switch_brightness() dereferences device->brightness or device->backlight. Fix this by calling cancel_delayed_work_sync() for each device's switch_brightness_work in acpi_video_bus_remove_notify_handler() after removing the notify handler that queues the work. This ensures the work completes before the memory is freed. [rjw: Changelog edit]	N/A	More Details
CVE-2025-66092	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bqworks Accordion Slider accordion-slider allows Stored XSS.This issue affects Accordion Slider: from n/a through <= 1.9.13.	N/A	More Details
CVE-2025-66095	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Iqonic Design KiviCare kivicare-clinic-management-system allows SQL Injection.This issue affects KiviCare: from n/a through <= 3.6.13.	N/A	More Details
CVE-2025-66096	Missing Authorization vulnerability in Imtiaz Rayhan Table Block by Tableberg tableberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Table Block by Tableberg: from n/a through <= 0.6.9.	N/A	More Details
CVE-2025-66106	Missing Authorization vulnerability in Essential Plugin Featured Post Creative featured-post-creative allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Featured Post Creative: from n/a through <= 1.5.5.	N/A	More Details
CVE-2025-66107	Missing Authorization vulnerability in Scott Paterson Subscriptions & Memberships for PayPal subscriptions-memberships-for-paypal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Subscriptions & Memberships for PayPal: from n/a through <= 1.1.7.	N/A	More Details
CVE-2025-66108	Missing Authorization vulnerability in Merlot Digital (by TNC) TNC Toolbox: Web Performance tnc-toolbox allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TNC Toolbox: Web Performance: from n/a through <= 2.0.4.	N/A	More Details
CVE-2025-66109	Missing Authorization vulnerability in octolize Cart Weight for WooCommerce woo-cart-weight allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cart Weight for WooCommerce: from n/a through <= 1.9.11.	N/A	More Details
CVE-	Missing Authorization vulnerability in bPlugins Tiktok Feed b-tiktok-feed allows		

2025-66110	Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tiktok Feed: from n/a through <= 1.0.22.	N/A	More Details
CVE-2025-66114	Missing Authorization vulnerability in theme funda Show Variations as Single Products Woocommerce woo-show-single-variations-shop-category allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Show Variations as Single Products Woocommerce: from n/a through <= 2.0.	N/A	More Details
CVE-2025-11931	Integer Underflow Leads to Out-of-Bounds Access in XChaCha20-Poly1305 Decrypt. This issue is hit specifically with a call to the function wc_XChaCha20Poly1305_Decrypt() which is not used with TLS connections, only from direct calls from an application.	N/A	More Details
CVE-2025-66115	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in MatrixAddons Easy Invoice easy-invoice allows PHP Local File Inclusion.This issue affects Easy Invoice: from n/a through <= 2.1.4.	N/A	More Details
CVE-2025-64483	Wazuh is a security detection, visibility, and compliance open source project. From version 4.9.0 to before 4.13.0, the Wazuh API – Agent Configuration in certain configurations allows authenticated users with read-only API roles to retrieve agent enrollment credentials through the /utils/configuration endpoint. These credentials can be used to register new agents within the same Wazuh tenant without requiring elevated permissions through the UI. This issue has been patched in version 4.13.0.	N/A	More Details
CVE-2025-54866	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.3.0 to before 4.13.0, a missing ACL on "C:\Program Files (x86)\ossec-agent\authd.pass" exposes the password to all "Authenticated Users" on the local machine. This issue has been patched in version 4.13.0.	N/A	More Details
CVE-2025-62608	MLX is an array framework for machine learning on Apple silicon. Prior to version 0.29.4, there is a heap buffer overflow in mlx::core::load() when parsing malicious NumPy .npy files. Attacker-controlled file causes 13-byte out-of-bounds read, leading to crash or information disclosure. This issue has been patched in version 0.29.4.	N/A	More Details
CVE-2025-62609	MLX is an array framework for machine learning on Apple silicon. Prior to version 0.29.4, there is a segmentation fault in mlx::core::load_gguf() when loading malicious GGUF files. Untrusted pointer from external gguflib library is dereferenced without validation, causing application crash. This issue has been patched in version 0.29.4.	N/A	More Details
CVE-2025-62626	Improper handling of insufficient entropy in the AMD CPUs could allow a local attacker to influence the values returned by the RDSEED instruction, potentially resulting in the consumption of insufficiently random values.	N/A	More Details
CVE-2025-64169	Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 3.7.0 to before 4.12.0, fim_alert() implementation does not check whether oldsum->md5 is NULL or not before dereferencing it. A compromised agent can cause a crash of analysisd by sending a specially crafted message to the wazuh manager. This issue has been patched in version 4.12.0.	N/A	More Details
CVE-2025-11935	With TLS 1.3 pre-shared key (PSK) a malicious or faulty server could ignore the request for PFS (perfect forward secrecy) and the client would continue on with the connection using PSK without PFS. This happened when a server responded to a ClientHello containing psk_dhe_ke without a key_share extension. The re-use of an authenticated PSK connection that on the clients side unexpectedly did not have PFS, reduces the security of the connection.	N/A	More Details
CVE-2025-65092	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.1, 5.4.3, and 5.3.4, when the ESP32-P4 uses its hardware JPEG decoder, the software parser lacks necessary validation checks. A specially crafted (malicious) JPEG image could exploit the parsing routine and trigger an out-of-bounds array access. This issue has been fixed in versions 5.5.2, 5.4.4, and 5.3.5. At time of publication versions 5.5.2, 5.4.4, and 5.3.5 have not been released but are fixed respectively in commits	N/A	More Details

	4b8f585, c79cb4d, and 34e2726.		
CVE-2025-65102	PJSIP is a free and open source multimedia communication library. Prior to version 2.16, Opus PLC may zero-fill the input frame as long as the decoder ptime, while the input frame length, which is based on stream ptime, may be less than that. This issue affects PJSIP users who use the Opus audio codec in receiving direction. The vulnerability can lead to unexpected application termination due to a memory overwrite. This issue has been patched in version 2.16.	N/A	More Details
CVE-2025-65106	LangChain is a framework for building agents and LLM-powered applications. From versions 0.3.79 and prior and 1.0.0 to 1.0.6, a template injection vulnerability exists in LangChain's prompt template system that allows attackers to access Python object internals through template syntax. This vulnerability affects applications that accept untrusted template strings (not just template variables) in ChatPromptTemplate and related prompt template classes. This issue has been patched in versions 0.3.80 and 1.0.7.	N/A	More Details
CVE-2025-65109	Minder is an open source software supply chain security platform. In Minder Helm version 0.20241106.3386+ref.2507dbf and Minder Go versions from 0.0.72 to 0.0.83, Minder users may fetch content in the context of the Minder server, which may include URLs which the user would not normally have access to. This issue has been patched in Minder Helm version 0.20250203.3849+ref.fdc94f0 and Minder Go version 0.0.84.	N/A	More Details
CVE-2025-65111	SpiceDB is an open source database system for creating and managing security-critical application permissions. Prior to version 1.47.1, if a schema includes the following characteristics: permission defined in terms of a union (+) and that union references the same relation on both sides (but one side arrows to a different permission). Then SpiceDB may have missing LookupResources results when checking the permission. This only affects LookupResources; other APIs calculate permissionship correctly. The issue is fixed in version 1.47.1.	N/A	More Details
CVE-2025-65953	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. Prior to version 0.22.5, a Heap-Use-After-Free (UAF) vulnerability exists in the TCP transport component of NanoMQ, which relies on the underlying NanoNNG library (specifically in src/sp/transport/mqtt/broker_tcp.c). The vulnerability is due to improper resource management and premature cleanup of message and pipe structures under specific malformed MQTTV5 retain message traffic conditions. This issue has been patched in version 0.22.5.	N/A	More Details