

Security Bulletin 19_February_2025

Generated on 19_February_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-2025-26615	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Path Traversal vulnerability was discovered in the WeGIA application, `examples.php` endpoint. This vulnerability could allow an attacker to gain unauthorized access to sensitive information stored in `config.php`. `config.php` contains information that could allow direct access to the database. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	10.0	More Details
CVE-2025-22654	Unrestricted Upload of File with Dangerous Type vulnerability in kodeshpa Simplified allows Using Malicious Files. This issue affects Simplified: from n/a through 1.0.6.	10.0	More Details
CVE-2025-24865	The administrative web interface of mySCADA myPRO Manager can be accessed without authentication which could allow an unauthorized attacker to retrieve sensitive information and upload files without the associated password.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13152	Authorization Bypass Through User-Controlled SQL Primary Key vulnerability in BSS Software Mobuy Online Machinery Monitoring Panel allows SQL Injection.This issue affects Mobuy Online Machinery Monitoring Panel: before 2.0.	10.0	More Details
CVE-2024-10960	The Brizy – Page Builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'storeUploads' function in all versions up to, and including, 2.6.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.9	More Details
CVE-2024-39327	Incorrect Access Control vulnerability in Atos Eviden IDRA before 2.6.1 could allow the possibility to obtain CA signing in an illegitimate way.	9.9	More Details
CVE-2025-22630	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in MarketingFire Widget Options allows OS Command Injection.This issue affects Widget Options: from n/a through 4.1.0.	9.9	More Details
CVE-2025-0867	The standard user uses the run as function to start the MEAC applications with administrative privileges. To ensure that the system can startup on its own, the credentials of the administrator were stored. Consequently, the EPC2 user can execute any command with administrative privileges. This allows a privilege escalation to the administrative level.	9.9	More Details
CVE-2024-56180	CWE-502 Deserialization of Untrusted Data at the eventmesh-meta-raft plugin module in Apache EventMesh master branch without release version on windows\linux\mac os e.g. platforms allows attackers to send controlled message and remote code execute via hessian deserialization rpc protocol. Users can use the code under the master branch in project repo or version 1.11.0 to fix this issue.	9.8	More Details
CVE-2025-1283	The Dingtian DT-R0 Series is vulnerable to an exploit that allows attackers to bypass login requirements by directly navigating to the main page.	9.8	More Details
CVE-2025-25067	mySCADA myPRO Manager is vulnerable to an OS command injection which could allow a remote attacker to execute arbitrary OS commands.	9.8	More Details
CVE-2025-1298	Logic vulnerability in the mobile application (com.transsion.carlcare) may lead to the risk of account takeover.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13513	The Oliver POS – A WooCommerce Point of Sale (POS) plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.4.2.3 via the logging functionality. This makes it possible for unauthenticated attackers to extract sensitive data including the plugin's clientToken, which in turn can be used to change user account information including emails and account type. This allows attackers to then change account passwords resulting in a complete site takeover. Version 2.4.2.3 disabled logging but left sites with existing log files vulnerable.	9.8	More Details
CVE-2025-1302	Versions of the package jsonpath-plus before 10.3.0 are vulnerable to Remote Code Execution (RCE) due to improper input sanitization. An attacker can execute arbitrary code on the system by exploiting the unsafe default usage of eval='safe' mode. Note: This is caused by an incomplete fix for [CVE-2024-21534] (https://security.snyk.io/vuln/SNYK-JS-JSONPATHPLUS-7945884).	9.8	More Details
CVE-2025-25388	A SQL Injection vulnerability was found in /admin/edit-propertytype.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the editid GET request parameter.	9.8	More Details
CVE-2024-12562	The s2Member Pro plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.4.12.16 via deserialization of untrusted input from the 's2member_pro_remote_op' vulnerable parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software. 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.	9.8	More Details
CVE-2025-1387	Orca HCM from LEARNING DIGITAL has an Improper Authentication vulnerability, allowing unauthenticated remote attackers to log in to the system as any user.	9.8	More Details
CVE-2024-13725	The Keap Official Opt-in Forms plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.0.1 via the service parameter. This makes it possible for unauthenticated attackers to include PHP files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where PHP files can be uploaded and included. If register_argc_argv is enabled on the server and pearcmd.php is installed, this issue might lead to Remote Code Execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-12860	The CarSpot – Dealership Wordpress Classified Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.4.3. This is due to the plugin not properly validating a token prior to updating a user's password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account.	9.8	More Details
CVE-2024-56000	Incorrect Privilege Assignment vulnerability in NotFound K Elements allows Privilege Escalation. This issue affects K Elements: from n/a through n/a.	9.8	More Details
CVE-2024-12213	The WP Job Board Pro plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.2.76. This is due to the plugin allowing a user to supply the 'role' field when registering. This makes it possible for unauthenticated attackers to register as an administrator on vulnerable sites.	9.8	More Details
CVE-2024-13421	The Real Estate 7 WordPress theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.5.1. This is due to the plugin not properly restricting the roles allowed to be selected during registration. This makes it possible for unauthenticated attackers to register a new administrative user account.	9.8	More Details
CVE-2025-26347	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/menu/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to edit user permissions via crafted HTTP requests.	9.8	More Details
CVE-2025-26359	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/accounts/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to reset user PINs via crafted HTTP requests.	9.8	More Details
CVE-2024-13365	The Security & Malware scan by CleanTalk plugin for WordPress is vulnerable to arbitrary file uploads due to the plugin uploading and extracting .zip archives when scanning them for malware through the checkUploadedArchive() function in all versions up to, and including, 2.149. 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-2025-1100	A CWE-259 "Use of Hard-coded Password" for the root account in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to execute arbitrary code with root privileges via SSH.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26339	A CWE-306 "Missing Authentication for Critical Function" in maxtime/handleRoute.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to affect the device confidentiality, integrity, or availability in multiple unspecified ways via crafted HTTP requests.	9.8	More Details
CVE-2025-26341	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/accounts/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to reset arbitrary user passwords via crafted HTTP requests.	9.8	More Details
CVE-2025-26342	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/accounts/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to create arbitrary users, including administrators, via crafted HTTP requests.	9.8	More Details
CVE-2025-26344	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/guest-mode/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to enable passwordless guest mode via crafted HTTP requests.	9.8	More Details
CVE-2025-26345	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/menu/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to edit user group permissions via crafted HTTP requests.	9.8	More Details
CVE-2024-13182	The WP Directorybox Manager plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.5. This is due to incorrect authentication in the 'wp_dp_parse_request' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator.	9.8	More Details
CVE-2025-25389	A SQL Injection vulnerability was found in /admin/forgot-password.php in Phpgurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the contactno POST request parameter.	9.8	More Details
CVE-2025-25349	PHPGurukul Daily Expense Tracker System v1.1 is vulnerable to SQL Injection in /dets/add-expense.php via the costitem parameter.	9.8	More Details
CVE-2025-25351	PHPGurukul Daily Expense Tracker System v1.1 is vulnerable to SQL Injection in /dets/add-expense.php via the dateexpense parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25286	Crayfish is a collection of Islandora 8 microservices, one of which, Homarus, provides FFmpeg as a microservice. Prior to Crayfish version 4.1.0, remote code execution may be possible in web-accessible installations of Homarus in certain configurations. The issue has been patched in `islandora/crayfish:4.1.0`. Some workarounds are available. The exploit requires making a request against the Homarus's `/convert` endpoint; therefore, the ability to exploit is much reduced if the microservice is not directly accessible from the Internet, so: Prevent general access from the Internet from hitting Homarus. Alternatively or additionally, configure auth in Crayfish to be more strongly required, such that requests with `Authorization` headers that do not validate are rejected before the problematic CLI interpolation occurs.	9.8	More Details
CVE-2025-0896	Orthanc server prior to version 1.5.8 does not enable basic authentication by default when remote access is enabled. This could result in unauthorized access by an attacker.	9.8	More Details
CVE-2024-10763	The Campress theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.35 via the 'campress_woocommerce_get_ajax_products' function. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included.	9.8	More Details
CVE-2024-7102	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.4 prior to 17.5.0 which allows an attacker to trigger a pipeline as another user under certain circumstances.	9.6	More Details
CVE-2025-25182	Stroom is a data processing, storage and analysis platform. A vulnerability exists starting in version 7.2-beta.53 and prior to versions 7.2.24, 7.3-beta.22, 7.4.4, and 7.5-beta.2 that allows authentication bypass to a Stroom system when configured with ALB and installed in a way that the application is accessible not through the ALB itself. This vulnerability may also allow for server-side request forgery which may lead to code execution or further privileges escalations when using the AWS metadata URL. This scenario assumes that Stroom must be configured to use ALB Authentication integration and the application is network accessible. The vulnerability has been fixed in versions 7.2.24, 7.3-beta.22, 7.4.4, and 7.5-beta.2.	9.4	More Details
CVE-2025-22290	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in enituretechnology LTL Freight Quotes - FreightQuote Edition allows SQL Injection. This issue affects LTL Freight Quotes - FreightQuote Edition: from n/a through 2.3.11.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26361	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/setup/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to factory reset the device via crafted HTTP requests.	9.1	More Details
CVE-2024-57971	DataSourceResource.java in the SpagoBI API support in Knowage Server in KNOWAGE before 8.1.30 does not ensure that java:comp/env/jdbc/ occurs at the beginning of a JNDI Name.	9.1	More Details
CVE-2022-31631	In PHP versions 8.0.* before 8.0.27, 8.1.* before 8.1.15, 8.2.* before 8.2.2 when using PDO::quote() function to quote user-supplied data for SQLite, supplying an overly long string may cause the driver to incorrectly quote the data, which may further lead to SQL injection vulnerabilities.	9.1	More Details
CVE-2025-24894	SPID.AspNetCore.Authentication is an AspNetCore Remote Authenticator for SPID. Authentication using Spid and CIE is based on the SAML2 standard which provides two entities: Identity Provider (IDP): the system that authenticates users and provides identity information (SAML affirmation) to the Service Provider, in essence, is responsible for the management of the credentials and identity of users; Service Provider (SP): the system that provides a service to the user and relies on the Identity Provider to authenticate the user, receives SAML assertions from the IdP to grant access to resources. The validation logic of the signature is central as it ensures that you cannot create a SAML response with arbitrary assertions and then impersonate other users. There is no guarantee that the first signature refers to the root object, it follows that if an attacker injects an item signed as the first element, all other signatures will not be verified. The only requirement is to have an XML element legitimately signed by the IdP, a condition that is easily met using the IdP's public metadata. An attacker could create an arbitrary SAML response that would be accepted by SPs using vulnerable SDKs, allowing him to impersonate any Spid and/or CIE user. This vulnerability has been addressed in version 3.4.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-24895	CIE.AspNetCore.Authentication is an AspNetCore Remote Authenticator for CIE 3.0. Authentication using Spid and CIE is based on the SAML2 standard which provides two entities: 1. Identity Provider (IDP): the system that authenticates users and provides identity information (SAML affirmation) to the Service Provider, in essence, is responsible for the management of the credentials and identity of users; 2. Service Provider (SP): the system that provides a service to the user and relies on the Identity Provider to authenticate the user, receives SAML assertions from the IdP to grant access to resources. The library cie-aspnetcore refers to the second entity, the SP, and implements the validation logic of SAML assertions within SAML responses. In affected versions there is no guarantee that the first signature refers to the root object, it follows that if an attacker injects an item signed as the first element, all other signatures will not be verified. The only requirement is to have an XML element legitimately signed by the IdP, a condition that is easily met using the IdP's public metadata. An attacker could create an arbitrary SAML response that would be accepted by SPs using vulnerable SDKs, allowing him to impersonate any Spid and/or CIE user. This issue has been addressed in version 2.1.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2025-1127	The vulnerability can be leveraged by an attacker to execute arbitrary code as an unprivileged user and/or modify the contents of any data on the filesystem.	9.1	More Details
CVE-2025-1270	Insecure direct object reference (IDOR) vulnerability in Anapi Group's h6web, allows an authenticated attacker to access other users' information by making a POST request and modifying the "pkrelated" parameter in the "/h6web/ha_datos_hermano.php" endpoint to refer to another user. In addition, the first request could also allow the attacker to impersonate other users. As a result, all requests made after exploitation of the IDOR vulnerability will be executed with the privileges of the impersonated user.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
------------	-------------	------------	-----------

CVE Number	Description	Base Score	Reference
CVE-2024-13677	The GetBookingsWP – Appointments Booking Calendar Plugin For WordPress plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.1.27. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for authenticated attackers, with subscriber-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	8.8	More Details
CVE-2025-26340	A CWE-321 "Use of Hard-coded Cryptographic Key" in the JWT signing in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to bypass the authentication via crafted HTTP requests.	8.8	More Details
CVE-2025-26156	A SQL Injection vulnerability was found in /shopping/track-orders.php in PHPGurukul Online Shopping Portal v2.1, which allows remote attackers to execute arbitrary code via orderid POST request parameter.	8.8	More Details
CVE-2024-13653	The ZoxPress - The All-In-One WordPress News Theme theme for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'backup_options' function in all versions up to, and including, 2.12.0. 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-2024-13852	The Option Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing nonce validation on the plugin_page() function. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	8.8	More Details
CVE-2024-57778	An issue in Orbe ONetView Roeador Onet-1200 Orbe 1680210096 allows a remote attacker to escalate privileges via the servers response from status code 500 to status code 200.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13714	The All-Images.ai – IA Image Bank and Custom Image creation plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the '_get_image_by_url' function in all versions up to, and including, 1.0.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-13636	The Brooklyn theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.9.9.2 via deserialization of untrusted input in the ot_decode function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	8.8	More Details
CVE-2025-26371	A CWE-862 "Missing Authorization" in maxprofile/user-groups/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to add users to groups via crafted HTTP requests.	8.8	More Details
CVE-2025-25745	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the Password parameter in the SetQuickVPNSettings module.	8.8	More Details
CVE-2025-26378	A CWE-862 "Missing Authorization" in maxprofile/users/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to reset passwords, including the ones of administrator accounts, via crafted HTTP requests.	8.8	More Details
CVE-2024-12296	The Apus Framework plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'import_page_options' function in all versions up to, and including, 2.3. 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 Number	Description	Base Score	Reference
CVE-2025-1340	A vulnerability classified as critical has been found in TOTOLINK X18 9.1.0cu.2024_B20220329. Affected is the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi. The manipulation as part of String leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-26511	Systems running the Instaclustr fork of Stratio's Cassandra-Lucene-Index plugin versions 4.0-rc1-1.0.0 through 4.0.16-1.0.0 and 4.1.2-1.0.0 through 4.1.8-1.0.0, installed into Apache Cassandra version 4.x, are susceptible to a vulnerability which when successfully exploited could allow authenticated Cassandra users to remotely bypass RBAC and escalate their privileges.	8.8	More Details
CVE-2024-34520	An authorization bypass vulnerability exists in the Mavenir SCE Application Provisioning Portal, version PORTAL-LBS-R_1_0_24_0, which allows an authenticated 'guest' user to perform unauthorized administrative actions, such as accessing the 'add user' feature, by bypassing client-side access controls.	8.8	More Details
CVE-2025-0556	In Progress® Telerik® Report Server, versions prior to 2025 Q1 (11.0.25.211) when using the older .NET Framework implementation, communication of non-sensitive information between the service agent process and app host process occurs over an unencrypted tunnel, which can be subjected to local network traffic sniffing.	8.8	More Details
CVE-2024-37355	Improper access control in some Intel(R) Graphics software may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2025-1244	A flaw was found in the Emacs text editor. Improper handling of custom "man" URI schemes allows attackers to execute arbitrary shell commands by tricking users into visiting a specially crafted website or an HTTP URL with a redirect.	8.8	More Details
CVE-2025-1389	Orca HCM from Learning Digital has a SQL Injection vulnerability, allowing attackers with regular privileges to inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2024-13315	The Shopwarden – Automated WooCommerce monitoring & testing plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.11. This is due to missing or incorrect nonce validation on the save_setting() function. This makes it possible for unauthenticated attackers to update arbitrary options and achieve privilege escalation via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0592	The vulnerability may allow a remote low privileged attacker to run arbitrary shell commands by manipulating the firmware file and uploading it to the device.	8.8	More Details
CVE-2025-1388	Orca HCM from LEARNING DIGITAL has an Arbitrary File Upload vulnerability, allowing remote attackers with regular privileges to upload and run web shells	8.8	More Details
CVE-2025-26369	A CWE-862 "Missing Authorization" in maxprofile/user-groups/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to add privileges to user groups via crafted HTTP requests.	8.8	More Details
CVE-2025-0593	The vulnerability may allow a remote low privileged attacker to run arbitrary shell commands by using lower-level functions to interact with the device.	8.8	More Details
CVE-2025-26375	A CWE-862 "Missing Authorization" in maxprofile/users/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to create users with arbitrary privileges via crafted HTTP requests.	8.8	More Details
CVE-2025-0376	An XSS vulnerability exists in GitLab CE/EE affecting all versions from 13.3 prior to 17.6.5, 17.7 prior to 17.7.4 and 17.8 prior to 17.8.2 that allows an attacker to execute unauthorized actions via a change page.	8.7	More Details
CVE-2025-22896	mySCADA myPRO Manager stores credentials in cleartext, which could allow an attacker to obtain sensitive information.	8.6	More Details
CVE-2025-22663	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in videowhisper Paid Videochat Turnkey Site allows Path Traversal. This issue affects Paid Videochat Turnkey Site: from n/a through 7.2.12.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25297	Label Studio is an open source data labeling tool. Prior to version 1.16.0, Label Studio's S3 storage integration feature contains a Server-Side Request Forgery (SSRF) vulnerability in its endpoint configuration. When creating an S3 storage connection, the application allows users to specify a custom S3 endpoint URL via the s3_endpoint parameter. This endpoint URL is passed directly to the boto3 AWS SDK without proper validation or restrictions on the protocol or destination. The vulnerability allows an attacker to make the application send HTTP requests to arbitrary internal services by specifying them as the S3 endpoint. When the storage sync operation is triggered, the application attempts to make S3 API calls to the specified endpoint, effectively making HTTP requests to the target service and returning the response in error messages. This SSRF vulnerability enables attackers to bypass network segmentation and access internal services that should not be accessible from the external network. The vulnerability is particularly severe because error messages from failed requests contain the full response body, allowing data exfiltration from internal services. Version 1.16.0 contains a patch for the issue.	8.6	More Details
CVE-2025-26819	Monero through 0.18.3.4 before ec74ff4 does not have response limits on HTTP server connections.	8.6	More Details
CVE-2025-24903	libsignal-service-rs is a Rust version of the libsignal-service-java library which implements the core functionality to communicate with Signal servers. Prior to commit 82d70f6720e762898f34ae76b0894b0297d9b2f8, any contact may forge a sync message, impersonating another device of the local user. The origin of sync messages is not checked. Patched libsignal-service can be found after commit 82d70f6720e762898f34ae76b0894b0297d9b2f8. The `Metadata` struct contains an additional `was_encrypted` field, which breaks the API, but should be easily resolvable. No known workarounds are available.	8.5	More Details
CVE-2024-12651	Exposed Dangerous Method or Function vulnerability in PTT Inc. HGS Mobile App allows Manipulating User-Controlled Variables.This issue affects HGS Mobile App: before 6.5.0.	8.5	More Details
CVE-2025-22639	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NotFound Distance Rate Shipping for WooCommerce allows Blind SQL Injection. This issue affects Distance Rate Shipping for WooCommerce: from n/a through 1.3.4.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-24904	libsignal-service-rs is a Rust version of the libsignal-service-java library which implements the core functionality to communicate with Signal servers. Prior to commit 82d70f6720e762898f34ae76b0894b0297d9b2f8, plaintext content envelopes could be injected by a server or a malicious client, and may have been able to bypass the end-to-end encryption and authentication. The vulnerability is fixed per 82d70f6720e762898f34ae76b0894b0297d9b2f8. The `Metadata` struct contains an additional `was_encrypted` field, which breaks the API, but should be easily resolvable. No known workarounds are available.	8.5	More Details
CVE-2025-26788	StrongKey FIDO Server before 4.15.1 treats a non-discoverable (namedcredential) flow as a discoverable transaction.	8.4	More Details
CVE-2025-1247	A flaw was found in Quarkus REST that allows request parameters to leak between concurrent requests if endpoints use field injection without a CDI scope. This vulnerability allows attackers to manipulate request data, impersonate users, or access sensitive information.	8.3	More Details
CVE-2025-23359	NVIDIA Container Toolkit for Linux contains a Time-of-Check Time-of-Use (TOCTOU) vulnerability when used with default configuration, where a crafted container image could gain access to the host file system. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	8.3	More Details
CVE-2025-25206	eLabFTW is an open source electronic lab notebook for research labs. Prior to version 5.1.15, an incorrect input validation could allow an authenticated user to read sensitive information, including login token or other content stored in the database. This could lead to privilege escalation if cookies are enabled (default setting). Users must upgrade to eLabFTW version 5.1.15 to receive a fix. No known workarounds are available.	8.3	More Details
CVE-2024-11343	In Progress® Telerik® Document Processing Libraries, versions prior to 2025 Q1 (2025.1.205), unzipping an archive can lead to arbitrary file system access.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26604	Discord-Bot-Framework-Kernel is a Discord bot framework built with interactions.py, featuring modular extension management and secure execution. Because of the nature of arbitrary user-submitted code execution, this allows user to execute potentially malicious code to perform damage or extract sensitive information. By loading the module containing the following code and run the command, the bot token can be extracted. Then the attacker can load a blocking module to sabotage the bot (DDoS attack) and the token can be used to make the fake bot act as the real one. If the bot has very high privilege, the attacker basically has full control before the user kicks the bot. Any Discord user that hosts Discord-Bot-Framework-Kernel before commit f0d9e70841a0e3170b88c4f8d562018ccd8e8b14 is affected. Users are advised to upgrade. Users unable to upgrade may attempt to limit their discord bot's access via configuration options.	8.3	More Details
CVE-2023-43758	Improper input validation in UEFI firmware for some Intel(R) processors may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2025-25205	Audiobookshelf is a self-hosted audiobook and podcast server. Starting in version 2.17.0 and prior to version 2.19.1, a flaw in the authentication bypass logic allows unauthenticated requests to match certain unanchored regex patterns in the URL. Attackers can craft URLs containing substrings like "/api/items/1/cover" in a query parameter (?r=/api/items/1/cover) to partially bypass authentication or trigger server crashes under certain routes. This could lead to information disclosure of otherwise protected data and, in some cases, a complete denial of service (server crash) if downstream code expects an authenticated user object. Version 2.19.1 contains a patch for the issue.	8.2	More Details
CVE-2023-31276	Heap-based buffer overflow in BMC Firmware for the Intel(R) Server Board S2600WF, Intel(R) Server Board S2600ST, Intel(R) Server Board S2600BP, before version 02.01.0017 and Intel(R) Server Board M50CYP and Intel(R) Server Board D50TNP before version R01.01.0009 may allow a privileged user to enable escalation of privilege via local access.	8.2	More Details
CVE-2024-38310	Improper access control in some Intel(R) Graphics Driver software installers may allow an authenticated user to potentially enable escalation of privilege via local access.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1094	Improper neutralization of quoting syntax in PostgreSQL libpq functions PQescapeLiteral(), PQescapeIdentifier(), PQescapeString(), and PQescapeStringConn() allows a database input provider to achieve SQL injection in certain usage patterns. Specifically, SQL injection requires the application to use the function result to construct input to psql, the PostgreSQL interactive terminal. Similarly, improper neutralization of quoting syntax in PostgreSQL command line utility programs allows a source of command line arguments to achieve SQL injection when client_encoding is BIG5 and server_encoding is one of EUC_TW or MULE_INTERNAL. Versions before PostgreSQL 17.3, 16.7, 15.11, 14.16, and 13.19 are affected.	8.1	More Details
CVE-2024-13556	The Affiliate Links: WordPress Plugin for Link Cloaking and Link Management plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.0.1 via deserialization of untrusted input from a file export. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	8.1	More Details
CVE-2024-12386	The WP Abstracts plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.3. This is due to missing nonce validation on multiple functions. This makes it possible for unauthenticated attackers to delete arbitrary accounts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.1	More Details
CVE-2025-26519	musl libc 0.9.13 through 1.2.5 before 1.2.6 has an out-of-bounds write vulnerability when an attacker can trigger iconv conversion of untrusted EUC-KR text to UTF-8.	8.1	More Details
CVE-2025-26368	A CWE-862 "Missing Authorization" in maxprofile/user-groups/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to remove user groups via crafted HTTP requests.	8.1	More Details
CVE-2024-13654	The ZoxPress - The All-In-One WordPress News Theme theme for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the 'reset_options' function in all versions up to, and including, 2.12.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary option values on the WordPress site. This can be leveraged to delete an option that would create an error on the site and deny service to legitimate users.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13656	The Click Mag - Viral WordPress News Magazine/Blog Theme theme for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the <code>propanel_of_ajax_callback()</code> function in all versions up to, and including, 3.6.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary option values on the WordPress site. This can be leveraged to delete an option that would create an error on the site and deny service to legitimate users.	8.1	More Details
CVE-2024-13684	The Reset plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6. This is due to missing or incorrect nonce validation on the <code>reset_db_page()</code> function. This makes it possible for unauthenticated attackers to reset several tables in the database like comments, themes, plugins, and more via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.1	More Details
CVE-2025-26377	A CWE-862 "Missing Authorization" in <code>maxprofile/users/routes.lua</code> in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to remove users via crafted HTTP requests.	8.1	More Details
CVE-2025-1146	CrowdStrike uses industry-standard TLS (transport layer security) to secure communications from the Falcon sensor to the CrowdStrike cloud. CrowdStrike has identified a validation logic error in the Falcon sensor for Linux, Falcon Kubernetes Admission Controller, and Falcon Container Sensor where our TLS connection routine to the CrowdStrike cloud can incorrectly process server certificate validation. This could allow an attacker with the ability to control network traffic to potentially conduct a man-in-the-middle (MiTM) attack. CrowdStrike identified this issue internally and released a security fix in all Falcon sensor for Linux, Falcon Kubernetes Admission Controller, and Falcon Container Sensor versions 7.06 and above. CrowdStrike identified this issue through our longstanding, rigorous security review process, which has been continually strengthened with deeper source code analysis and ongoing program enhancements as part of our commitment to security resilience. CrowdStrike has no indication of any exploitation of this issue in the wild. CrowdStrike has leveraged its world class threat hunting and intelligence capabilities to actively monitor for signs of abuse or usage of this flaw and will continue to do so. Windows and Mac sensors are not affected by this.	8.1	More Details
CVE-2025-26343	A CWE-1390 "Weak Authentication" in the PIN authentication mechanism in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to brute-force user PINs via multiple crafted HTTP requests.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13770	The Puzzles WP Magazine / Review with Store WordPress Theme + RTL theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.2.4 via deserialization of untrusted input 'view_more_posts' AJAX action. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. The developer opted to remove the software from the repository, so an update is not available and it is recommended to find a replacement software.	8.1	More Details
CVE-2024-13800	The ConvertPlus plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the 'cp_dismiss_notice' AJAX endpoint in all versions up to, and including, 3.5.30. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update option values to '1' on the WordPress site. This can be leveraged to update an option that would create an error on the site and deny service to legitimate users or be used to set some values to true such as registration.	8.1	More Details
CVE-2025-1058	CWE-494: Download of Code Without Integrity Check vulnerability exists that could render the device inoperable when malicious firmware is downloaded.	8.1	More Details
CVE-2025-1070	CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists that could render the device inoperable when a malicious file is downloaded.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-24888	The SecureDrop Client is a desktop application for journalists to communicate with sources and work with submissions on the SecureDrop Workstation. Prior to version 0.14.1, a malicious SecureDrop Server could obtain code execution on the SecureDrop Client virtual machine (`sd-app`). SecureDrop Server itself has multiple layers of built-in hardening, and is a dedicated physical machine exposed on the internet only via Tor hidden services for the Source and Journalist interfaces, and optionally via remote SSH access over another Tor hidden service. A newsroom's SecureDrop Workstation communicates only with its own dedicated SecureDrop Server. The SecureDrop Client runs in a dedicated Qubes virtual machine, named `sd-app`, as part of the SecureDrop Workstation. The private OpenPGP key used to decrypt submissions and replies is stored in a separate virtual machine and never accessed directly. The vulnerability lies in the code responsible for downloading replies. The filename of the reply is obtained from the `Content-Disposition` HTTP header and used to write the encrypted reply on disk. Note that filenames are generated and sanitized server-side, and files are downloaded in an encrypted format, so a remote attacker who has not achieved server compromise, such as one posing as a source, could not craft the HTTP response necessary for this attack. While the filename is later checked to guard against path traversal before being moved into the Client's data storage directory, the file has already been written to a potentially arbitrary location. In this case, `safe_move()` would detect the path traversal and fail, leaving the original downloaded file in the attacker-chosen directory. Code execution can be gained by writing an autostart file in `/home/user/.config/autostart/`. Version 0.14.1 fixes the issue. As of time of publication, there is no known evidence of exploitation in the wild. This attack requires a previously compromised SecureDrop Server.	8.1	More Details
CVE-2025-22656	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Oscar Alvarez Cookie Monster allows PHP Local File Inclusion. This issue affects Cookie Monster: from n/a through 1.2.2.	8.1	More Details
CVE-2024-51505	An issue was discovered in Atos Eviden IDRA before 2.7.1. A highly trusted role (Config Admin) could leverage a race condition to escalate privileges.	8.0	More Details
CVE-2023-48267	Improper buffer restrictions in some Intel(R) System Security Report and System Resources Defense firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.9	More Details
CVE-2024-32941	NULL pointer dereference for some Intel(R) MLC software before version v3.11b may allow an authenticated user to potentially enable denial of service via local access.	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-12673	An improper privilege vulnerability was reported in a BIOS customization feature of Lenovo Vantage on SMB notebook devices which could allow a local attacker to elevate privileges on the system. This vulnerability only affects Vantage installed on these devices: * Lenovo V Series (Gen 5) * ThinkBook 14 (Gen 6, 7) * ThinkBook 16 (Gen 6, 7) * ThinkPad E Series (Gen 1)	7.8	More Details
CVE-2025-0327	CWE-269: Improper Privilege Management vulnerability exists for two services (of which one managing audit trail data and the other acting as server managing client request) that could cause a loss of Confidentiality, Integrity and Availability of engineering workstation when an attacker with standard privilege modifies the executable path of the windows services. To be exploited, services need to be restarted.	7.8	More Details
CVE-2024-57951	In the Linux kernel, the following vulnerability has been resolved: hrtimers: Handle CPU state correctly on hotplug Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE: Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once. This round-trip reveals another issue; cpu_base.online is not set to 1 after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer(). Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case. Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag. [tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback]	7.8	More Details
CVE-2025-21703	In the Linux kernel, the following vulnerability has been resolved: netem: Update sch->q.qlen before qdisc_tree_reduce_backlog() qdisc_tree_reduce_backlog() notifies parent qdisc only if child qdisc becomes empty, therefore we need to reduce the backlog of the child qdisc before calling it. Otherwise it would miss the opportunity to call cops->qlen_notify(), in the case of DRR, it resulted in UAF since DRR uses ->qlen_notify() to maintain its active list.	7.8	More Details
CVE-2024-39805	Insufficient verification of data authenticity in some Intel(R) DSA software before version 23.4.39 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-21103	Dell NetWorker Management Console, version(s) 19.11 through 19.11.0.3 & Versions prior to 19.10.0.7 contain(s) an improper neutralization of server-side vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability and run arbitrary code on the server.	7.8	More Details
CVE-2024-31858	Out-of-bounds write for some Intel(R) QuickAssist Technology software before version 2.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2025-0591	Out-of-bounds Read vulnerability (CWE-125) was found in CX-Programmer. Attackers may be able to read sensitive information or cause an application crash by abusing this vulnerability.	7.8	More Details
CVE-2025-0332	In Progress® Telerik® UI for WinForms, versions prior to 2025 Q1 (2025.1.211), using the improper limitation of a target path can lead to decompressing an archive's content into a restricted directory.	7.8	More Details
CVE-2025-24928	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSnprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. NOTE: this is similar to CVE-2017-9047.	7.8	More Details
CVE-2024-12251	In Progress® Telerik® UI for WinUI versions prior to 2025 Q1 (3.0.0), a command injection attack is possible through improper neutralization of hyperlink elements.	7.8	More Details
CVE-2024-56171	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a use-after-free in xmlSchemaIDCFillNodeTables and xmlSchemaBubbleIDCNodeTables in xmlschemas.c. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-21700	In the Linux kernel, the following vulnerability has been resolved: net: sched: Disallow replacing of child qdisc from one parent to another Lion Ackermann was able to create a UAF which can be abused for privilege escalation with the following script Step 1. create root qdisc <pre>tc qdisc add dev lo root handle 1:0 drr</pre> step2. a class for packet aggregation <pre>do demonstrate uaf tc class add dev lo classid 1:1 drr</pre> step3. a class for nesting <pre>tc class add dev lo classid 1:2 drr</pre> step4. a class to graft qdisc to tc <pre>class add dev lo classid 1:3 drr</pre> step5. tc qdisc add dev lo parent 1:1 handle 2:0 plug limit 1024 step6. tc qdisc add dev lo parent 1:2 handle 3:0 drr step7. tc class add dev lo classid 3:1 drr step 8. tc qdisc add dev lo parent 3:1 handle 4:0 pfifo step 9. Display the class/qdisc layout <pre>tc class ls dev lo class drr 1:1 root leaf 2: quantum 64Kb class drr 1:2 root leaf 3: quantum 64Kb class drr 3:1 root leaf 4: quantum 64Kb tc qdisc ls qdisc drr 1: dev lo root refcnt 2 qdisc plug 2: dev lo parent 1:1 qdisc pfifo 4: dev lo parent 3:1 limit 1000p qdisc drr 3: dev lo parent 1:2</pre> step10. trigger the bug <=== prevented by this patch <pre>tc qdisc replace dev lo parent 1:3 handle 4:0</pre> step 11. Redisplay again the qdiscs/classes <pre>tc class ls dev lo class drr 1:1 root leaf 2: quantum 64Kb class drr 1:2 root leaf 3: quantum 64Kb class drr 1:3 root leaf 4: quantum 64Kb class drr 3:1 root leaf 4: quantum 64Kb tc qdisc ls qdisc drr 1: dev lo root refcnt 2 qdisc plug 2: dev lo parent 1:1 qdisc pfifo 4: dev lo parent 3:1 refcnt 2 limit 1000p qdisc drr 3: dev lo parent 1:2</pre> Observe that a) parent for 4:0 does not change despite the replace request. There can only be one parent. b) refcount has gone up by two for 4:0 and c) both class 1:3 and 3:1 are pointing to it. Step 12. send one packet to plug <pre>echo "" socat -u STDIN UDP4-DATAGRAM:127.0.0.1:8888,priority=\$((0x10001))</pre> step13. send one packet to the grafted fifo <pre>echo "" socat -u STDIN UDP4-DATAGRAM:127.0.0.1:8888,priority=\$((0x10003))</pre> step14. lets trigger the uaf <pre>tc class delete dev lo classid 1:3 tc class delete dev lo classid 1:1</pre> The semantics of "replace" is for a del/add _on the same node_ and not a delete from one node(3:1) and add to another node (1:3) as in step10. While we could "fix" with a more complex approach there could be consequences to expectations so the patch takes the preventive approach of "disallow such config". Joint work with Lion Ackermann <nnamrec@gmail.com>	7.8	More Details
CVE-2024-38307	Improper input validation in the firmware for some Intel(R) AMT and Intel(R) Standard Manageability may allow an authenticated user to potentially enable denial of service via network access.	7.7	More Details
CVE-2025-26520	Cacti through 1.2.29 allows SQL injection in the template function in host_templates.php via the graph_template parameter. NOTE: this issue exists because of an incomplete fix for CVE-2024-54146.	7.6	More Details
CVE-2025-26755	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in jgwhite33 WP Airbnb Review Slider allows Blind SQL Injection. This issue affects WP Airbnb Review Slider: from n/a through 3.9.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-12013	A CWE-1392 "Use of Default Credentials" was discovered affecting the 130.8005 TCP/IP Gateway running firmware version 12h. The device exposes an FTP server with default and easy-to-guess admin credentials. A remote attacker capable of interacting with the FTP server could gain access and perform changes over resources exposed by the service such as configuration files where password hashes are saved or where network settings are stored.	7.6	More Details
CVE-2024-12011	A CWE-126 "Buffer Over-read" was discovered affecting the 130.8005 TCP/IP Gateway running firmware version 12h. The information disclosure can be triggered by leveraging a memory leak affecting the web server. A remote unauthenticated attacker can exploit this vulnerability in order to leak valid authentication tokens from the process memory associated to users currently logged to the system and bypass the authentication mechanism.	7.6	More Details
CVE-2025-25901	A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11, triggered by the dnsserver1 and dnsserver2 parameters at /userRpm/WanSlaacCfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	7.5	More Details
CVE-2024-41917	Time-of-check time-of-use race condition for some Intel(R) Battery Life Diagnostic Tool software before version 2.4.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2025-26365	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/setup/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to enable front panel authentication via crafted HTTP requests.	7.5	More Details
CVE-2024-13681	The Unicode theme for WordPress is vulnerable to arbitrary file read due to insufficient input validation in the 'unicode_admin_get_oembed' function in all versions up to, and including, 2.9.1.6. This makes it possible for unauthenticated attackers to read arbitrary files on the server.	7.5	More Details
CVE-2023-49618	Improper buffer restrictions in some Intel(R) System Security Report and System Resources Defense firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-49615	Improper input validation in some Intel(R) System Security Report and System Resources Defense firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-49603	Race condition in some Intel(R) System Security Report and System Resources Defense firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-24861	An attacker may inject commands via specially-crafted post requests.	7.5	More Details
CVE-2023-34440	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2025-25281	An attacker may modify the URL to discover sensitive information about the target network.	7.5	More Details
CVE-2024-13488	The LTL Freight Quotes - Estes Edition plugin for WordPress is vulnerable to SQL Injection via the 'dropship_edit_id' and 'edit_id' parameters in all versions up to, and including, 3.3.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-26473	The Mojave Inverter uses the GET method for sensitive information.	7.5	More Details
CVE-2024-28127	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-29214	Improper input validation in UEFI firmware CseVariableStorageSmm for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2025-25283	parse-duraton is software that allows users to convert a human readable duration to milliseconds. Versions prior to 2.1.3 are vulnerable to an event loop delay due to the CPU-bound operation of resolving the provided string, from a 0.5ms and up to ~50ms per one operation, with a varying size from 0.01 MB and up to 4.3 MB respectively, and an out of memory that would crash a running Node.js application due to a string size of roughly 10 MB that utilizes unicode characters. Version 2.1.3 contains a patch.	7.5	More Details
CVE-2024-13622	The File Uploads Addon for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.7.1 via the 'uploads' directory. This makes it possible for unauthenticated attackers to extract sensitive data stored insecurely in the /wp-content/uploads directory which can contain file attachments uploaded by customers.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31155	Improper buffer restrictions in the UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2025-22657	Missing Authorization vulnerability in Vito Peleg Atarim allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Atarim: from n/a through 4.0.9.	7.5	More Details
CVE-2025-25199	go-crypto-winnative Go crypto backend for Windows using Cryptography API: Next Generation (CNG). Prior to commit f49c8e1379ea4b147d5bff1b3be5b0ff45792e41, calls to `cng.TLS1PRF` don't release the key handle, producing a small memory leak every time. Commit f49c8e1379ea4b147d5bff1b3be5b0ff45792e41 contains a fix for the issue. The fix is included in versions 1.23.6-2 and 1.22.12-2 of the Microsoft build of go, as well as in the pseudoversion 0.0.0-20250211154640-f49c8e1379ea of the `github.com/microsoft/go-crypto-winnative` Go package.	7.5	More Details
CVE-2025-26366	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/setup/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to disable front panel authentication via crafted HTTP requests.	7.5	More Details
CVE-2024-24582	Improper input validation in XmlCli feature for UEFI firmware for some Intel(R) processors may allow privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2025-26364	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/setup/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to disable an authentication profile server via crafted HTTP requests.	7.5	More Details
CVE-2025-1059	CWE-770: Allocation of Resources Without Limits or Throttling vulnerability exists that could cause communications to stop when malicious packets are sent to the webserver of the device.	7.5	More Details
CVE-2025-26363	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/setup/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to enable an authentication profile server via crafted HTTP requests.	7.5	More Details
CVE-2024-13531	The ShipEngine Shipping Quotes plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' parameter in all versions up to, and including, 1.0.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13477	The LTL Freight Quotes – Unishippers Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' parameter in all versions up to, and including, 2.5.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-13480	The LTL Freight Quotes – For Customers of FedEx Freight plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 3.4.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-13528	The Customer Email Verification for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.9.5. This is due to the presence of a shortcode that will generate a confirmation link with a placeholder email. This makes it possible for authenticated attackers, with Contributor-level access and above, to generate a verification link for any unverified user and log into the account. The 'Fine tune placement' option must be enabled in the plugin settings in order to exploit the vulnerability.	7.5	More Details
CVE-2024-13532	The Small Package Quotes – Purolator Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 3.6.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-13490	The LTL Freight Quotes – XPO Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 4.3.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13475	The Small Package Quotes – UPS Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' parameter in all versions up to, and including, 4.5.16 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-2024-13473	The LTL Freight Quotes – Worldwide Express Edition plugin for WordPress is vulnerable to SQL Injection via the 'dropship_edit_id' and 'edit_id' parameter in all versions up to, and including, 5.0.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-13435	The Ebook Downloader plugin for WordPress is vulnerable to SQL Injection via the 'download' parameter in all versions up to, and including, 1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-12315	The Export All Posts, Products, Orders, Refunds & Users plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.9.3 via the exports directory. This makes it possible for unauthenticated attackers to extract sensitive data stored insecurely in the /wp-content/uploads/smack_uci_uploads/exports/ directory which can contain information like exported user data.	7.5	More Details
CVE-2022-26083	Generation of weak initialization vector in an Intel(R) IPP Cryptography software library before version 2021.5 may allow an unauthenticated user to potentially enable information disclosure via local access.	7.5	More Details
CVE-2025-1060	CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists that could result in the exposure of data when network traffic is being sniffed by an attacker.	7.5	More Details
CVE-2024-51376	Directory Traversal vulnerability in yeqifu carRental v.1.0 allows a remote attacker to obtain sensitive information via the file/downloadFile.action?path= component.	7.5	More Details
CVE-2025-25898	A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11 via the pskSecret parameter at /userRpm/WlanSecurityRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13600	The Majestic Support – The Leading-Edge Help Desk & Customer Support Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.5 via the 'majesticsupportdata' directory. This makes it possible for unauthenticated attackers to extract sensitive data stored insecurely in the /wp-content/uploads/majesticsupportdata directory which can contain file attachments included in support tickets.	7.5	More Details
CVE-2023-31345	Improper input validation in the SMM handler may allow a privileged attacker to overwrite SMRAM, potentially leading to arbitrary code execution.	7.5	More Details
CVE-2025-26362	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/setup/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to set an arbitrary authentication profile server via crafted HTTP requests.	7.5	More Details
CVE-2025-25997	Directory Traversal vulnerability in FeMiner wms v.1.0 allows a remote attacker to obtain sensitive information via the databak.php component.	7.5	More Details
CVE-2025-25994	SQL Injection vulnerability in FeMiner wms wms 1.0 allows a remote attacker to obtain sensitive information via the parameters date1, date2, id.	7.5	More Details
CVE-2025-25897	A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11 via the 'ip' parameter at /userRpm/WanStaticIpV6CfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	7.5	More Details
CVE-2024-0112	NVIDIA Jetson AGX Orin™ and NVIDIA IGX Orin software contain a vulnerability where an attacker can cause an improper input validation issue by escalating certain permissions to a limited degree. A successful exploit of this vulnerability might lead to code execution, denial of service, data corruption, information disclosure, or escalation of privilege.	7.5	More Details
CVE-2024-13606	The JS Help Desk – The Ultimate Help Desk & Support Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.8.8 via the 'jssupportticketdata' directory. This makes it possible for unauthenticated attackers to extract sensitive data stored insecurely in the /wp-content/uploads/jssupportticketdata directory which can contain file attachments included in support tickets.	7.5	More Details
CVE-2024-41168	Use after free in some Intel(R) PROSet/Wireless WiFi and Killer®, Wi-Fi software for Windows before version 23.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39356	NULL pointer dereference in some Intel(R) PROSet/Wireless WiFi and Killerâ„¢ WiFi software for Windows before version 23.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	7.4	More Details
CVE-2024-13345	The Avada Builder plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.11.13. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-57964	Insecure Loading of Dynamic Link Libraries have been discovered in HVAC Energy Saving Program, which could allow local attackers to potentially disclose information or execute arbitray code on affected systems. This issue affects HVAC Energy Saving Program:.	7.3	More Details
CVE-2024-11347	Integer Overflow or Wraparound vulnerability in Lexmark International CX, XC, CS, et. Al. (Postscript interpreter modules) allows Forced Integer Overflow.The vulnerability can be leveraged by an attacker to execute arbitrary code as an unprivileged user.	7.3	More Details
CVE-2024-13797	The PressMart - Modern Elementor WooCommerce WordPress Theme theme for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.2.16. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-13346	The Avada Website Builder For WordPress & WooCommerce theme for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 7.11.13. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2023-29164	Improper access control in BMC Firmware for the Intel(R) Server Board S2600WF, Intel(R) Server Board S2600ST, Intel(R) Server Board S2600BP, before version 02.01.0017 and Intel(R) Server Board M50CYP and Intel(R) Server Board D50TNP before version R01.01.0009 may allow an authenticated user to enable escalation of privilege via local access.	7.3	More Details
CVE-2024-57963	Insecure Loading of Dynamic Link Libraries have been discovered in USB-CONVERTERCABLE DRIVER, which could allow local attackers to potentially disclose information or execute arbitray code on affected systems. This issue affects USB-CONVERTERCABLE DRIVER:.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1338	A vulnerability was found in NUUO Camera up to 20250203. It has been declared as critical. This vulnerability affects the function print_file of the file /handle_config.php. The manipulation of the argument log leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-8893	Use of Hard-coded Credentials vulnerability in GoodWe Technologies Co., Ltd. GW1500-XS allows anyone in physical proximity to the device to fully access the web interface of the inverter via Wi-Fi.This issue affects GW1500-XS: 1.1.2.1.	7.3	More Details
CVE-2024-11346	: Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in Lexmark International CX, XC, CS, et. Al. (Postscript interpreter modules) allows Resource Injection.This issue affects CX, XC, CS, et. Al.: from 001.001:0 through 081.231, from *.*.P001 through *.*.P233, from *.*.P001 through *.*.P759, from *.*.P001 through *.*.P836.	7.3	More Details
CVE-2024-13603	The Wise Forms WordPress plugin through 1.2.0 does not sanitise and escape some of its settings, which could allow unauthenticated users to perform Stored Cross-Site Scripting attacks via malicious form submissions.	7.3	More Details
CVE-2025-1355	A vulnerability was found in needyamin Library Card System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /signup.php of the component Add Picture. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-11345	A heap-based memory vulnerability has been identified in the Postscript interpreter in various Lexmark devices. The vulnerability can be leveraged by an attacker to execute arbitrary code.	7.3	More Details
CVE-2024-11344	A type confusion vulnerability has been identified in the Postscript interpreter in various Lexmark devices. The vulnerability can be leveraged by an attacker to execute arbitrary code.	7.3	More Details
CVE-2024-52500	Missing Authorization vulnerability in monetagwp Monetag Official Plugin allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Monetag Official Plugin: from n/a through 1.1.3.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0924	The WP Activity Log plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'message' parameter in all versions up to, and including, 5.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-25356	A SQL Injection vulnerability was found in /admin/bwdates-reports-details.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the " todate" POST request parameter.	7.2	More Details
CVE-2025-25357	A SQL Injection vulnerability was found in /admin/contactus.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the email POST request parameter.	7.2	More Details
CVE-2025-26349	A CWE-23 "Relative Path Traversal" in the file upload mechanism in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to overwrite arbitrary files via crafted HTTP requests.	7.2	More Details
CVE-2024-13704	The Super Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'st_user_title' parameter in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-0817	The FormCraft plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.9.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	7.2	More Details
CVE-2025-25387	A SQL Injection vulnerability was found in /admin/manage-propertytype.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the propertytype POST request parameter.	7.2	More Details
CVE-2025-26354	A CWE-35 "Path Traversal" in maxtime/api/database/database.lua (copy endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to overwrite sensitive files via crafted HTTP requests.	7.2	More Details
CVE-2025-26356	A CWE-35 "Path Traversal" in maxtime/api/database/database.lua (setActive endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to overwrite sensitive files via crafted HTTP requests.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0521	The Post SMTP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the from and subject parameter in all versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-36262	Race condition in some Intel(R) System Security Report and System Resources Defense firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2025-25354	A SQL Injection was found in /admin/admin-profile.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the contactnumber POST request parameter.	7.2	More Details
CVE-2025-25352	A SQL Injection vulnerability was found in /admin/aboutus.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the pagetitle POST request parameter.	7.2	More Details
CVE-2025-22962	A critical remote code execution (RCE) vulnerability exists in the web-based management interface of GatesAir Maxiva UAXT, VAXT transmitters when debugging mode is enabled. An attacker with a valid session ID (sess_id) can send specially crafted POST requests to the /json endpoint, enabling arbitrary command execution on the underlying system. This vulnerability can lead to full system compromise, including unauthorized access, privilege escalation, and potentially full device takeover.	7.2	More Details
CVE-2024-55904	IBM DevOps Deploy 8.0 through 8.0.1.4, 8.1 through 8.1.0.0 / IBM UrbanCode Deploy 7.0 through 7.0.5.25, 7.1 through 7.1.2.21, 7.2 through 7.2.3.14, and 7.3 through 7.3.2.9 could allow a remote privileged authenticated attacker to execute arbitrary commands on the system by sending specially crafted input containing special elements.	7.2	More Details
CVE-2025-0511	The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 2.11.9 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-2024-12314	The Rapid Cache plugin for WordPress is vulnerable to Cache Poisoning in all versions up to, and including, 1.2.3. This is due to plugin storing HTTP headers in the cached data. This makes it possible for unauthenticated attackers to poison the cache with custom HTTP headers that may be unsanitized which can lead to Cross-Site Scripting.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25355	A SQL Injection vulnerability was found in /admin/bwdates-reports-details.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the fromdate POST request parameter.	7.2	More Details
CVE-2025-26578	Cross-Site Request Forgery (CSRF) vulnerability in mathieuhays Simple Documentation allows Stored XSS. This issue affects Simple Documentation: from n/a through 1.2.8.	7.1	More Details
CVE-2025-26577	Cross-Site Request Forgery (CSRF) vulnerability in daxiawp DX-auto-publish allows Stored XSS. This issue affects DX-auto-publish: from n/a through 1.2.	7.1	More Details
CVE-2025-24592	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SysBasics Customize My Account for WooCommerce allows Reflected XSS. This issue affects Customize My Account for WooCommerce: from n/a through 2.8.22.	7.1	More Details
CVE-2025-26582	Cross-Site Request Forgery (CSRF) vulnerability in Blackbam TinyMCE Advanced qTranslate fix editor problems allows Stored XSS. This issue affects TinyMCE Advanced qTranslate fix editor problems: from n/a through 1.0.0.	7.1	More Details
CVE-2025-26547	Cross-Site Request Forgery (CSRF) vulnerability in nagarjunsonti My Login Logout Plugin allows Stored XSS. This issue affects My Login Logout Plugin: from n/a through 2.4.	7.1	More Details
CVE-2025-26549	Cross-Site Request Forgery (CSRF) vulnerability in pa1 WP Html Page Sitemap allows Stored XSS. This issue affects WP Html Page Sitemap: from n/a through 2.2.	7.1	More Details
CVE-2025-26550	Cross-Site Request Forgery (CSRF) vulnerability in Kunal Shivale Global Meta Keyword & Description allows Stored XSS. This issue affects Global Meta Keyword & Description: from n/a through 2.3.	7.1	More Details
CVE-2025-26551	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sureshdsk Bootstrap collapse allows Stored XSS. This issue affects Bootstrap collapse: from n/a through 1.0.4.	7.1	More Details
CVE-2025-26571	Cross-Site Request Forgery (CSRF) vulnerability in wibiya Wibiya Toolbar allows Cross Site Request Forgery. This issue affects Wibiya Toolbar: from n/a through 2.0.	7.1	More Details
CVE-2024-46910	An authenticated user can perform XSS and potentially impersonate another user. This issue affects Apache Atlas versions 2.3.0 and earlier. Users are recommended to upgrade to version 2.4.0, which fixes the issue.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26552	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in badrHan Naver Syndication V2 allows Stored XSS. This issue affects Naver Syndication V2: from n/a through 0.8.3.	7.1	More Details
CVE-2025-26580	Cross-Site Request Forgery (CSRF) vulnerability in CompleteWebResources Page/Post Specific Social Share Buttons allows Stored XSS. This issue affects Page/Post Specific Social Share Buttons: from n/a through 2.1.	7.1	More Details
CVE-2025-26562	Cross-Site Request Forgery (CSRF) vulnerability in Shambhu Patnaik RSS Filter allows Stored XSS. This issue affects RSS Filter: from n/a through 1.2.	7.1	More Details
CVE-2025-26570	Cross-Site Request Forgery (CSRF) vulnerability in uamv Glance That allows Cross Site Request Forgery. This issue affects Glance That: from n/a through 4.9.	7.1	More Details
CVE-2025-26572	Cross-Site Request Forgery (CSRF) vulnerability in jesseheap WP PHPList allows Cross Site Request Forgery. This issue affects WP PHPList: from n/a through 1.7.	7.1	More Details
CVE-2025-24836	With a specially crafted Python script, an attacker could send continuous startMeasurement commands over an unencrypted Bluetooth connection to the affected device. This would prevent the device from connecting to a clinician's app to take patient readings and ostensibly flood it with requests, resulting in a denial-of-service condition.	7.1	More Details
CVE-2025-26569	Cross-Site Request Forgery (CSRF) vulnerability in callmeforsox Post Thumbs allows Stored XSS. This issue affects Post Thumbs: from n/a through 1.5.	7.1	More Details
CVE-2025-26568	Cross-Site Request Forgery (CSRF) vulnerability in jensmueller Easy Amazon Product Information allows Stored XSS. This issue affects Easy Amazon Product Information: from n/a through 4.0.1.	7.1	More Details
CVE-2025-26543	Cross-Site Request Forgery (CSRF) vulnerability in Pukhraj Suthar Simple Responsive Menu allows Stored XSS. This issue affects Simple Responsive Menu: from n/a through 2.1.	7.1	More Details
CVE-2025-23428	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound QMean – WordPress Did You Mean allows Reflected XSS. This issue affects QMean – WordPress Did You Mean: from n/a through 2.0.	7.1	More Details
CVE-2025-26370	A CWE-862 "Missing Authorization" in maxprofile/user-groups/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to remove privileges from user groups via crafted HTTP requests.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-23748	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Singsys -Awesome Gallery allows Reflected XSS. This issue affects Singsys -Awesome Gallery: from n/a through 1.0.	7.1	More Details
CVE-2025-22705	Cross-Site Request Forgery (CSRF) vulnerability in godthor Disqus Popular Posts allows Reflected XSS. This issue affects Disqus Popular Posts: from n/a through 2.1.1.	7.1	More Details
CVE-2025-23750	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devbunchuk Custom Widget Creator allows Reflected XSS. This issue affects Custom Widget Creator: from n/a through 1.0.5.	7.1	More Details
CVE-2025-23840	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webjema WP-NOTCAPTCHA allows Reflected XSS. This issue affects WP-NOTCAPTCHA: from n/a through 1.3.1.	7.1	More Details
CVE-2024-57259	sqfs_search_dir in Das U-Boot before 2025.01-rc1 exhibits an off-by-one error and resultant heap memory corruption for squashfs directory listing because the path separator is not considered in a size calculation.	7.1	More Details
CVE-2024-57256	An integer overflow in ext4fs_read_symlink in Das U-Boot before 2025.01-rc1 occurs for zalloc (adding one to an le32 variable) via a crafted ext4 filesystem with an inode size of 0xffffffff, resulting in a malloc of zero and resultant memory overwrite.	7.1	More Details
CVE-2025-23751	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Think201 Data Dash allows Reflected XSS. This issue affects Data Dash: from n/a through 1.2.3.	7.1	More Details
CVE-2025-26768	Cross-Site Request Forgery (CSRF) vulnerability in what3words what3words Address Field allows Stored XSS. This issue affects what3words Address Field: from n/a through 4.0.15.	7.1	More Details
CVE-2025-24614	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in agileLogix Post Timeline allows Reflected XSS. This issue affects Post Timeline: from n/a through 2.3.9.	7.1	More Details
CVE-2025-23845	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ERA404 ImageMeta allows Reflected XSS. This issue affects ImageMeta: from n/a through 1.1.2.	7.1	More Details
CVE-2025-26759	Cross-Site Request Forgery (CSRF) vulnerability in alexvtn Content Snippet Manager allows Stored XSS. This issue affects Content Snippet Manager: from n/a through 1.1.5.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-24615	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fatcatapps Analytics Cat allows Reflected XSS. This issue affects Analytics Cat: from n/a through 1.1.2.	7.1	More Details
CVE-2025-23786	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DuoGeek Email to Download allows Reflected XSS. This issue affects Email to Download: from n/a through 3.1.0.	7.1	More Details
CVE-2025-24616	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UIUX Lab Uix Page Builder allows Reflected XSS. This issue affects Uix Page Builder: from n/a through 1.7.3.	7.1	More Details
CVE-2025-23653	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Form To Online Booking allows Reflected XSS. This issue affects Form To Online Booking: from n/a through 1.0.	7.1	More Details
CVE-2025-23742	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Podamibe Nepal Podamibe Twilio Private Call allows Reflected XSS. This issue affects Podamibe Twilio Private Call: from n/a through 1.0.1.	7.1	More Details
CVE-2025-23431	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Envato Affiliater allows Reflected XSS. This issue affects Envato Affiliater: from n/a through 1.2.4.	7.1	More Details
CVE-2025-23474	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mike Martel Live Dashboard allows Reflected XSS. This issue affects Live Dashboard: from n/a through 0.3.3.	7.1	More Details
CVE-2025-23646	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt Brooks Library Instruction Recorder allows Reflected XSS. This issue affects Library Instruction Recorder: from n/a through 1.1.4.	7.1	More Details
CVE-2025-23651	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Scroll Top allows Reflected XSS. This issue affects Scroll Top: from n/a through 1.3.3.	7.1	More Details
CVE-2024-57258	Integer overflows in memory allocation in Das U-Boot before 2025.01-rc1 occur for a crafted squashfs filesystem via sbrk, via request2size, or because ptrdiff_t is mishandled on x86_64.	7.1	More Details
CVE-2025-23650	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in razvypp Tidy.ro allows Reflected XSS. This issue affects Tidy.ro: from n/a through 1.3.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-23655	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Contact Form 7 – Paystack Add-on allows Reflected XSS. This issue affects Contact Form 7 – Paystack Add-on: from n/a through 1.2.3.	7.1	More Details
CVE-2025-23648	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wjharil AdsMiddle allows Reflected XSS. This issue affects AdsMiddle: from n/a through 1.0.	7.1	More Details
CVE-2025-23647	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ariagle WP-Clap allows Reflected XSS. This issue affects WP-Clap: from n/a through 1.5.	7.1	More Details
CVE-2025-23598	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in craig.edmunds@gmail.com Recip.ly allows Reflected XSS. This issue affects Recip.ly: from n/a through 1.1.8.	7.1	More Details
CVE-2025-23492	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CantonBolo WordPress 淘宝客插件 allows Reflected XSS. This issue affects WordPress 淘宝客插件: from n/a through 1.1.2.	7.1	More Details
CVE-2025-23657	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WordPress-to-candidate for Salesforce CRM allows Reflected XSS. This issue affects WordPress-to-candidate for Salesforce CRM: from n/a through 1.0.1.	7.1	More Details
CVE-2025-23571	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Internal Links Generator allows Reflected XSS. This issue affects Internal Links Generator: from n/a through 3.51.	7.1	More Details
CVE-2025-23568	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fredsted WP Login Attempt Log allows Reflected XSS. This issue affects WP Login Attempt Log: from n/a through 1.3.	7.1	More Details
CVE-2025-23658	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tauhidul Alam Advanced Angular Contact Form allows Reflected XSS. This issue affects Advanced Angular Contact Form: from n/a through 1.1.0.	7.1	More Details
CVE-2025-23525	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kvvaradha Kv Compose Email From Dashboard allows Reflected XSS. This issue affects Kv Compose Email From Dashboard: from n/a through 1.1.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-23523	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hoststreamsell HSS Embed Streaming Video allows Reflected XSS. This issue affects HSS Embed Streaming Video: from n/a through 3.23.	7.1	More Details
CVE-2025-22680	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Ad Inserter Pro allows Reflected XSS. This issue affects Ad Inserter Pro: from n/a through 2.7.39.	7.1	More Details
CVE-2025-24617	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter allows Reflected XSS. This issue affects AcyMailing SMTP Newsletter: from n/a through n/a.	7.1	More Details
CVE-2025-23787	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Easy Bet allows Reflected XSS. This issue affects Easy Bet: from n/a through 1.0.7.	7.1	More Details
CVE-2024-11629	In Progress® Telerik® Document Processing Libraries, versions prior to 2025 Q1 (2025.1.205), using .NET Standard 2.0, the contents of a file at an arbitrary path can be exported to RTF.	7.1	More Details
CVE-2025-24566	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomáš Groulík Intro Tour Tutorial DeepPresentation allows Reflected XSS. This issue affects Intro Tour Tutorial DeepPresentation: from n/a through 6.5.2.	7.1	More Details
CVE-2025-24565	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saleswonder Team Tobias WP2LEADS allows Reflected XSS. This issue affects WP2LEADS: from n/a through 3.3.3.	7.1	More Details
CVE-2025-24564	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aviplugins.com Contact Form With Shortcode allows Reflected XSS. This issue affects Contact Form With Shortcode: from n/a through 4.2.5.	7.1	More Details
CVE-2025-24558	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks allows Reflected XSS. This issue affects CRM Perks: from n/a through 1.1.5.	7.1	More Details
CVE-2025-0937	Nomad Community and Nomad Enterprise ("Nomad") event stream configured with a wildcard namespace can bypass the ACL Policy allowing reads on other namespaces.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25198	mailcow: dockerized is an open source groupware/email suite based on docker. Prior to version 2025-01a, a vulnerability in mailcow's password reset functionality allows an attacker to manipulate the `Host HTTP` header to generate a password reset link pointing to an attacker-controlled domain. This can lead to account takeover if a user clicks the poisoned link. Version 2025-01a contains a patch. As a workaround, deactivate the password reset functionality by clearing `Notification email sender` and `Notification email subject` under System -> Configuration -> Options -> Password Settings.	7.1	More Details
CVE-2025-26545	Cross-Site Request Forgery (CSRF) vulnerability in shisuh Related Posts Line-up-Exactly by Milliard allows Stored XSS. This issue affects Related Posts Line-up-Exactly by Milliard: from n/a through 0.0.22.	7.1	More Details
CVE-2025-24554	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in awcode AWcode Toolkit allows Reflected XSS. This issue affects AWcode Toolkit: from n/a through 1.0.14.	7.1	More Details
CVE-2025-23905	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Johannes van Poelgeest Admin Options Pages allows Reflected XSS. This issue affects Admin Options Pages: from n/a through 0.9.7.	7.1	More Details
CVE-2024-57254	An integer overflow in sqfs_inode_size in Das U-Boot before 2025.01-rc1 occurs in the symlink size calculation via a crafted squashfs filesystem.	7.1	More Details
CVE-2025-23788	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Easy Filter allows Reflected XSS. This issue affects Easy Filter: from n/a through 1.10.	7.1	More Details
CVE-2025-23857	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Essential WP Real Estate allows Reflected XSS. This issue affects Essential WP Real Estate: from n/a through 1.1.3.	7.1	More Details
CVE-2025-23853	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in michelem NoFollow Free allows Reflected XSS. This issue affects NoFollow Free: from n/a through 1.6.3.	7.1	More Details
CVE-2024-57255	An integer overflow in sqfs_resolve_symlink in Das U-Boot before 2025.01-rc1 occurs via a crafted squashfs filesystem with an inode size of 0xffffffff, resulting in a malloc of zero and resultant memory overwrite.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-23851	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Coronavirus (COVID-19) Outbreak Data Widgets allows Reflected XSS. This issue affects Coronavirus (COVID-19) Outbreak Data Widgets: from n/a through 1.1.1.	7.1	More Details
CVE-2025-24700	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xylus Themes WP Event Aggregator allows Reflected XSS. This issue affects WP Event Aggregator: from n/a through 1.8.2.	7.1	More Details
CVE-2025-26372	A CWE-862 "Missing Authorization" in maxprofile/user-groups/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to remove users from groups via crafted HTTP requests.	7.1	More Details
CVE-2025-23789	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tahminajannat URL Shortener Conversion Tracking AB Testing WooCommerce allows Reflected XSS. This issue affects URL Shortener Conversion Tracking AB Testing WooCommerce: from n/a through 9.0.2.	7.1	More Details
CVE-2025-24641	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rickonline_nl Better WishList API allows Stored XSS. This issue affects Better WishList API: from n/a through 1.1.3.	7.1	More Details
CVE-2025-23790	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wassereimer Easy Code Placement allows Reflected XSS. This issue affects Easy Code Placement: from n/a through 18.11.	7.1	More Details
CVE-2025-24692	Missing Authorization vulnerability in Michael Revellin-Clerc Bulk Menu Edit allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Bulk Menu Edit: from n/a through 1.3.	7.1	More Details
CVE-2025-24699	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company WP Coder allows Cross-Site Scripting (XSS). This issue affects WP Coder: from n/a through 3.6.	7.1	More Details
CVE-2025-24688	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brandtoss WP Mailster allows Reflected XSS. This issue affects WP Mailster: from n/a through 1.8.20.0.	7.1	More Details
CVE-2025-22286	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in enituretechnology LTL Freight Quotes - Worldwide Express Edition allows Reflected XSS. This issue affects LTL Freight Quotes - Worldwide Express Edition: from n/a through 5.0.21.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-22284	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in enituretechnology LTL Freight Quotes – Unishippers Edition allows Reflected XSS. This issue affects LTL Freight Quotes – Unishippers Edition: from n/a through 2.5.8.	7.1	More Details
CVE-2024-44044	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Oshine Modules allows Reflected XSS. This issue affects Oshine Modules: from n/a through n/a.	7.1	More Details
CVE-2025-23652	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Add custom content after post allows Reflected XSS. This issue affects Add custom content after post: from n/a through 1.0.	7.1	More Details
CVE-2025-1353	A vulnerability was found in Kong Insomnia up to 10.3.0 and classified as critical. This issue affects some unknown processing in the library profapi.dll. The manipulation leads to untrusted search path. An attack has to be approached locally. The complexity of an attack is rather high. The exploitation is known to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2025-25305	Home Assistant Core is an open source home automation that puts local control and privacy first. Affected versions are subject to a potential man-in-the-middle attacks due to missing SSL certificate verification in the project codebase and used third-party libraries. In the past, ` aiohttp-session`/` request` had the parameter `verify_ssl` to control SSL certificate verification. This was a boolean value. In ` aiohttp` 3.0, this parameter was deprecated in favor of the `ssl` parameter. Only when `ssl` is set to `None` or provided with a correct configured SSL context the standard SSL certificate verification will happen. When migrating integrations in Home Assistant and libraries used by Home Assistant, in some cases the `verify_ssl` parameter value was just moved to the new `ssl` parameter. This resulted in these integrations and 3rd party libraries using `request.ssl = True`, which unintentionally turned off SSL certificate verification and opened up a man-in-the-middle attack vector. This issue has been addressed in version 2024.1.6 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	7.0	More Details
CVE-2025-22480	Dell SupportAssist OS Recovery versions prior to 5.5.13.1 contain a symbolic link attack vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary file deletion and Elevation of Privileges.	7.0	More Details
CVE-2024-39328	Insecure Permissions in Atos Eviden IDRA and IDCA before 2.7.0. A highly trusted role (Config Admin) could exceed their configuration privileges in a multi-partition environment and access some confidential data. Data integrity and availability is not at risk.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37600	An issue was discovered in Mercedes Benz NTG (New Telematics Generation) 6 through 2021. A possible stack buffer overflow in the Service Broker service affects NTG 6 head units. To perform this attack, physical access to Ethernet pins of the head unit base board is needed. With a static IP address, an attacker can connect via the internal network to the Service Broker service. With prepared HTTP requests, an attacker can cause the Service-Broker service to fail.	6.8	More Details
CVE-2025-26465	A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.	6.8	More Details
CVE-2024-0145	NVIDIA nvJPEG2000 library contains a vulnerability where an attacker can cause a heap-based buffer overflow issue by means of a specially crafted JPEG2000 file. A successful exploit of this vulnerability might lead to code execution and data tampering.	6.8	More Details
CVE-2024-0144	NVIDIA nvJPEG2000 library contains a vulnerability where an attacker can cause a buffer overflow issue by means of a specially crafted JPEG2000 file. A successful exploit of this vulnerability might lead to data tampering.	6.8	More Details
CVE-2024-0143	NVIDIA nvJPEG2000 library contains a vulnerability where an attacker can cause an out-of-bounds write issue by means of a specially crafted JPEG2000 file. A successful exploit of this vulnerability might lead to code execution and data tampering.	6.8	More Details
CVE-2024-0142	NVIDIA nvJPEG2000 library contains a vulnerability where an attacker can cause an out-of-bounds write issue by means of a specially crafted JPEG2000 file. A successful exploit of this vulnerability might lead to code execution and data tampering.	6.8	More Details
CVE-2024-21830	Uncontrolled search path in some Intel(R) VPL software before version 2023.4.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-32938	Uncontrolled search path for some Intel(R) MPI Library for Windows software before version 2021.13 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-32942	Incorrect default permissions for some Intel(R) DSA installer for Windows before version 24.2.19.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-39284	Uncontrolled search path for some Intel(R) Advisor software before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36280	Uncontrolled search path for some Intel(R) High Level Synthesis Compiler software before version 24.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-39365	Uncontrolled search path for the FPGA Support Package for the Intel(R) oneAPI DPC++/C++ Compiler software for Windows before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-39372	Uncontrolled search path for the Intel(R) XTU software for Windows before version 7.14.2.14 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-39813	Uncontrolled search path for some EPCT software before version 1.42.8.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-29223	Uncontrolled search path for some Intel(R) QuickAssist Technology software before version 2.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-45781	A flaw was found in grub2. When reading a symbolic link's name from a UFS filesystem, grub2 fails to validate the string length taken as an input. The lack of validation may lead to a heap out-of-bounds write, causing data integrity issues and eventually allowing an attacker to circumvent secure boot protections.	6.7	More Details
CVE-2024-42405	Uncontrolled search path for some Intel(R) Quartus(R) Prime Software before version 23.1.1 Patch 1.01std may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-36283	Uncontrolled search path for the Intel(R) Thread Director Visualizer software before version 1.0.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-42419	Incorrect default permissions for some Intel(R) GPA and Intel(R) GPA Framework software installers may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-42492	Uncontrolled search path element in some BIOS and System Firmware Update Package for Intel(R) Server M50FCP family before version R01.02.0002 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-47006	Uncontrolled search path for the Intel(R) RealSense D400 Series Universal Windows Platform (UWP) Driver for Windows(R) 10 all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45774	A flaw was found in grub2. A specially crafted JPEG file can cause the JPEG parser of grub2 to incorrectly check the bounds of its internal buffers, resulting in an out-of-bounds write. The possibility of overwriting sensitive information to bypass secure boot protections is not discarded.	6.7	More Details
CVE-2024-24852	Uncontrolled search path in some Intel(R) Ethernet Adapter Complete Driver Pack install before versions 29.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-45776	When reading the language .mo file in grub_mofile_open(), grub2 fails to verify an integer overflow when allocating its internal buffer. A crafted .mo file may lead the buffer size calculation to overflow, leading to out-of-bound reads and writes. This flaw allows an attacker to leak sensitive data or overwrite critical data, possibly circumventing secure boot protections.	6.7	More Details
CVE-2024-47935	Improper Validation of Integrity Check Value vulnerability in TXOne Networks StellarProtect (Legacy Mode), StellarEnforce, and Safe Lock allows an attacker to escalate their privileges in the victim's device. The attacker needs to hijack the DLL file in advance. This issue affects StellarProtect (Legacy Mode): before 3.2; StellarEnforce: before 3.2; Safe Lock: from 3.0.0 before 3.1.1076. *Note: StellarProtect (Legacy Mode) is the new name for StellarEnforce, they are the same product.	6.7	More Details
CVE-2024-36291	Uncontrolled search path for some Intel(R) Chipset Software Installation Utility before version 10.1.19867.8574 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2025-26574	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Moch Amir Google Drive WP Media allows Stored XSS. This issue affects Google Drive WP Media: from n/a through 2.4.4.	6.5	More Details
CVE-2024-56477	IBM Power Hardware Management Console V10.3.1050.0 could allow an authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	6.5	More Details
CVE-2024-13369	The Tour Master - Tour Booking, Travel, Hotel plugin for WordPress is vulnerable to time-based SQL Injection via the 'review_id' parameter in all versions up to, and including, 5.3.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-57725	An issue in the Arcadyan Livebox Fibra PRV3399B_B_LT allows a remote or local attacker to modify the GPON link value without authentication, causing an internet service disruption via the /firstconnection.cgi endpoint.	6.5	More Details
CVE-2024-13595	The Simple Signup Form plugin for WordPress is vulnerable to SQL Injection via the 'id' attribute of the 'ssf' shortcode in all versions up to, and including, 1.6.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing 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-2024-9601	The Qubely – Advanced Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' and 'UniqueID' parameter in all versions up to, and including, 1.8.12 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.	6.5	More Details
CVE-2024-52895	IBM i 7.4 and 7.5 is vulnerable to a database access denial of service caused by a bypass of a database capabilities restriction check. A privileged bad actor can remove or otherwise impact database infrastructure files resulting in incorrect behavior of software products that rely upon the database.	6.5	More Details
CVE-2025-26558	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mkkmail Aparat Responsive allows DOM-Based XSS. This issue affects Aparat Responsive: from n/a through 1.3.	6.5	More Details
CVE-2024-13691	The Uncode theme for WordPress is vulnerable to arbitrary file read due to insufficient input validation in the 'uncode_recordMedia' function in all versions up to, and including, 2.9.1.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary files on the server.	6.5	More Details
CVE-2025-23771	Missing Authorization vulnerability in Murali Push Notification for Post and BuddyPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Push Notification for Post and BuddyPress: from n/a through 2.11.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0821	Bit Assist plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 1.5.2 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 Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-23766	Missing Authorization vulnerability in ashamil OPSI Israel Domestic Shipments allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects OPSI Israel Domestic Shipments: from n/a through 2.6.6.	6.5	More Details
CVE-2025-23534	Missing Authorization vulnerability in Mark Winiarski WPLingo allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WPLingo: from n/a through 1.1.2.	6.5	More Details
CVE-2025-26567	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in farjana55 Font Awesome WP allows DOM-Based XSS. This issue affects Font Awesome WP: from n/a through 1.0.	6.5	More Details
CVE-2025-24567	Insertion of Sensitive Information Into Sent Data vulnerability in brandtoss WP Mailster allows Retrieve Embedded Sensitive Data. This issue affects WP Mailster: from n/a through 1.8.16.0.	6.5	More Details
CVE-2025-26539	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in petkivim Embed Google Map allows Stored XSS. This issue affects Embed Google Map: from n/a through 3.2.	6.5	More Details
CVE-2025-26376	A CWE-862 "Missing Authorization" in maxprofile/users/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to modify user data via crafted HTTP requests.	6.5	More Details
CVE-2025-26352	A CWE-35 "Path Traversal" in the template deletion mechanism in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to delete sensitive files via crafted HTTP requests.	6.5	More Details
CVE-2024-49589	Foundry Artifacts was found to be vulnerable to a Denial Of Service attack due to disk being potentially filled up based on an user supplied argument (size).	6.5	More Details
CVE-2024-42410	Improper input validation in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable denial of service via local access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-23975	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Botnet Attack Blocker allows Stored XSS. This issue affects Botnet Attack Blocker: from n/a through 2.0.0.	6.5	More Details
CVE-2025-22689	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Levan Tarbor Forex Calculators allows Stored XSS. This issue affects Forex Calculators: from n/a through 1.3.6.	6.5	More Details
CVE-2024-39797	Improper access control in some drivers for Intel(R) Ethernet Connection I219 Series before version 12.19.1.39 may allow an authenticated user to potentially enable denial of service via local access.	6.5	More Details
CVE-2025-26373	A CWE-862 "Missing Authorization" in maxprofile/users/routes.lua (user endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to enumerate users via crafted HTTP requests.	6.5	More Details
CVE-2024-39355	Improper handling of physical or environmental conditions in some Intel(R) Processors may allow an authenticated user to enable denial of service via local access.	6.5	More Details
CVE-2025-26374	A CWE-862 "Missing Authorization" in maxprofile/users/routes.lua (users endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to enumerate users via crafted HTTP requests.	6.5	More Details
CVE-2024-39279	Insufficient granularity of access control in UEFI firmware in some Intel(R) processors may allow a authenticated user to potentially enable denial of service via local access.	6.5	More Details
CVE-2024-12379	A denial of service vulnerability in GitLab CE/EE affecting all versions from 14.1 prior to 17.6.5, 17.7 prior to 17.7.4, and 17.8 prior to 17.8.2 allows an attacker to impact the availability of GitLab via unbounded symbol creation via the scopes parameter in a Personal Access Token.	6.5	More Details
CVE-2025-26766	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VaultDweller Leyka allows Stored XSS. This issue affects Leyka: from n/a through 3.31.8.	6.5	More Details
CVE-2024-36293	Improper access control in the EDECCSSA user leaf function for some Intel(R) Processors with Intel(R) SGX may allow an authenticated user to potentially enable denial of service via local access.	6.5	More Details
CVE-2024-36274	Out-of-bounds write in the Intel(R) 800 Series Ethernet Driver for Intel(R) Ethernet Adapter Complete Driver Pack before versions 29.1 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-22676	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in upcasted AWS S3 for WordPress Plugin – Upcasted allows Stored XSS. This issue affects AWS S3 for WordPress Plugin – Upcasted: from n/a through 3.0.3.	6.5	More Details
CVE-2025-22289	Missing Authorization vulnerability in NotFound LTL Freight Quotes – Unishippers Edition allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects LTL Freight Quotes – Unishippers Edition: from n/a through 2.5.8.	6.5	More Details
CVE-2024-13525	The Customer Email Verification for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.9.4 via Shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including emails as well as hashed passwords of any user.	6.5	More Details
CVE-2025-27016	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in awsm.in Drivr Lite – Google Drive Plugin allows Stored XSS. This issue affects Drivr Lite – Google Drive Plugin: from n/a through 1.0.1.	6.5	More Details
CVE-2025-26538	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan Rossiter Prezi Embedder allows Stored XSS. This issue affects Prezi Embedder: from n/a through 2.1.	6.5	More Details
CVE-2024-13752	The WP Project Manager – Task, team, and project management plugin featuring kanban board and gantt charts plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check in the '/pm/v2/settings/notice' endpoint all versions up to, and including, 2.6.17. This makes it possible for authenticated attackers, with Subscriber-level access and above, to cause a persistent denial of service condition.	6.5	More Details
CVE-2025-22650	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Erez Hadas-Sonnenschein Smartarget allows Stored XSS. This issue affects Smartarget: from n/a through 1.4.	6.5	More Details
CVE-2025-0822	Bit Assist plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.2 via the fileID Parameter. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-26761	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HashThemes Easy Elementor Addons allows DOM-Based XSS. This issue affects Easy Elementor Addons: from n/a through 2.1.5.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26355	A CWE-35 "Path Traversal" in maxtime/api/database/database.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to delete sensitive files via crafted HTTP requests.	6.5	More Details
CVE-2025-26767	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Qubely - Advanced Gutenberg Blocks allows Stored XSS. This issue affects Qubely - Advanced Gutenberg Blocks: from n/a through 1.8.12.	6.5	More Details
CVE-2025-0001	Abacus ERP is versions older than 2024.210.16036, 2023.205.15833, 2022.105.15542 are affected by an authenticated arbitrary file read vulnerability.	6.5	More Details
CVE-2025-26772	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Detheme DethemeKit For Elementor allows Stored XSS. This issue affects DethemeKit For Elementor: from n/a through 2.1.8.	6.5	More Details
CVE-2025-26771	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks - Gutenberg based Page Builder allows Stored XSS. This issue affects SKT Blocks - Gutenberg based Page Builder: from n/a through 1.7.	6.5	More Details
CVE-2025-26770	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Waymark allows Stored XSS. This issue affects Waymark: from n/a through 1.5.0.	6.5	More Details
CVE-2025-0816	CWE-20: Improper Input Validation vulnerability exists that could cause Denial-of-Service of the product when malicious IPV6 packets are sent to the device.	6.5	More Details
CVE-2025-0815	CWE-20: Improper Input Validation vulnerability exists that could cause Denial-of-Service of the product when malicious ICMPV6 packets are sent to the device.	6.5	More Details
CVE-2025-26769	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webilia Inc. Vertex Addons for Elementor allows Stored XSS. This issue affects Vertex Addons for Elementor: from n/a through 1.2.0.	6.5	More Details
CVE-2024-47265	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in encrypted share umount functionality in Synology Active Backup for Business before 2.7.1-13234, 2.7.1-23234 and 2.7.1-3234 allows remote authenticated users to write specific files via unspecified vectors.	6.5	More Details
CVE-2025-26754	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Timeline Block allows Stored XSS. This issue affects Timeline Block: from n/a through 1.1.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0714	The vulnerability existed in the password storage of Mobateks MobaXterm below 25.0. MobaXTerm uses an initialization vector (IV) that is generated by encrypting null bytes with a derivate of the users master key. As both the master key is static, and AES ECB produces the same output with the same input the IV for AES CFB is always the same. The static IV makes it easier to obtain sensitive information and decrypt data if the data is stored at rest.	6.5	More Details
CVE-2024-13500	The WP Project Manager – Task, team, and project management plugin featuring kanban board and gantt charts plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.6.17 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-1414	Memory safety bugs present in Firefox 135. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135.0.1.	6.5	More Details
CVE-2024-13456	The Easy Quiz Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wqt-question' shortcode in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-0805	The Mortgage Calculator / Loan Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mlcalc' shortcode in all versions up to, and including, 1.5.20 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-12813	The Open Hours – Easy Opening Hours plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'open-hours-current-status' shortcode in all versions up to, and including, 1.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13575	The Web Stories Enhancer – Level Up Your Web Stories plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'web_stories_enhancer' shortcode in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13701	The Liveticker (by stklcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'liveticker' shortcode in all versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13465	The aBlocks – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the "Table Of Content" Block, specifically in the "markerView" attribute, in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-11895	The Online Payments – Get Paid with PayPal, Square & Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 3.20.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-0622	A flaw was found in command/gpg. In some scenarios, hooks created by loaded modules are not removed when the related module is unloaded. This flaw allows an attacker to force grub2 to call the hooks once the module that registered it was unloaded, leading to a use-after-free vulnerability. If correctly exploited, this vulnerability may result in arbitrary code execution, eventually allowing the attacker to bypass secure boot protections.	6.4	More Details
CVE-2024-11746	The Discover the Best Woocommerce Product Brands Plugin for WordPress – Woocommerce Brands Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'product_brand' shortcode in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-12525	The Easy MLS Listings Import plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'homeasap-featured-listings' shortcode in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13743	The Wonder Video Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wonderplugin_video shortcode in all versions up to, and including, 2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13501	The WP-FormAssembly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'formassembly' shortcode in all versions up to, and including, 2.0.11 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10322	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 2.6.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-13735	The HurryTimer – An Scarcity and Urgency Countdown Timer for WordPress & WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.11.2 due to insufficient input sanitization and output escaping of a campaign name. 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-2025-0506	The Rise Blocks – A Complete Gutenberg Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the titleTag parameter in all versions up to, and including, 3.6 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-2024-54160	dashboards-reporting (aka Dashboards Reports) before 2.19.0.0, as shipped in OpenSearch before 2.19, allows XSS because Markdown is not sanitized when previewing a header or footer.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13464	The Library Bookshelves plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bookshelf' shortcode in all versions up to, and including, 5.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13665	The Admire Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'space' shortcode in all versions up to, and including, 1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13769	The Puzzles WP Magazine / Review with Store WordPress Theme + RTL theme for WordPress is vulnerable to Stored Cross-Site Scripting due to a missing capability check on the 'theme_options_ajax_post_action' AJAX action in all versions up to, and including, 4.2.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings and inject malicious web scripts. The developer opted to remove the software from the repository, so an update is not available and it is recommended to find a replacement software.	6.4	More Details
CVE-2024-13459	The FuseDesk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'fusedesk_newcase' shortcode in all versions up to, and including, 6.6.1 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-2024-13658	The NGG Smart Image Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'hr_SIS_nextgen_searchbox' shortcode in all versions up to, and including, 3.2.1 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-2024-13573	The Zigaform – Form Builder Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zgfm_rfvar' shortcode in all versions up to, and including, 7.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13395	The Threepress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'threepress' shortcode in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output 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-2024-13563	The Front End Users plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's forgot-password shortcode in all versions up to, and including, 3.2.30 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-2024-13576	The Gumlet Video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gumlet' shortcode in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13577	The CATS Job Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catsone' shortcode in all versions up to, and including, 2.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13587	The Zigaform – Price Calculator & Cost Estimation Form Builder Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zgfm_fvar' shortcode in all versions up to, and including, 7.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13565	The Simple Map No Api plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter in all versions up to, and including, 1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13588	The Simplebooklet PDF Viewer and Embedder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'simplebooklet' shortcode in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13644	The DethemeKit For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's De Gallery widget in all versions up to, and including, 2.1.8 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-2024-13227	The Rank Math SEO – AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Rank Math API in all versions up to, and including, 1.0.235 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-2024-13579	The WP-Asambleas plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'polls_popup' shortcode in all versions up to, and including, 2.85.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13578	The WP-BibTeX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'WpBibTeX' shortcode in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-1005	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Accordion widget in all versions up to, and including, 3.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3303	An issue was discovered in GitLab EE affecting all versions starting from 16.0 prior to 17.6.5, starting from 17.7 prior to 17.7.4, and starting from 17.8 prior to 17.8.2, which allows an attacker to exfiltrate contents of a private issue using prompt injection.	6.4	More Details
CVE-2024-13582	The Simple Pricing Tables For WPBakery Page Builder(Formerly Visual Composer) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wdo_simple_pricing_table_free' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-13581	The Simple Charts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'simple_chart' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-0837	The Puzzles theme for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 4.2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-23421	An attacker could obtain firmware files and reverse engineer their intended use leading to loss of confidentiality and integrity of the hardware devices enabled by the Qardio iOS and Android applications.	6.4	More Details
CVE-2025-1186	A vulnerability was found in dayrui XunRuiCMS up to 4.6.4. It has been declared as critical. This vulnerability affects unknown code of the file /Control/Api/Api.php. The manipulation of the argument thumb leads to deserialization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1200	A vulnerability was found in SourceCodester Best Church Management Software 1.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/app/slider_crud.php. The manipulation of the argument del_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-22698	Missing Authorization vulnerability in Ability, Inc Accessibility Suite by Online ADA allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accessibility Suite by Online ADA: from n/a through 4.16.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1229	A vulnerability classified as critical was found in olajowon Loggrove up to e428fac38cc480f011afcb1d8ce6c2bad378ddd6. Affected by this vulnerability is an unknown functionality of the file /read/?page=1&logfile=eee&match=. The manipulation of the argument path leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the 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-2025-1374	A vulnerability classified as critical has been found in code-projects Real Estate Property Management System 1.0. This affects an unknown part of the file /search.php. The manipulation of the argument StateName/CityName/AreaName/CatId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1183	A vulnerability has been found in CodeZips Gym Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /dashboard/admin/more-userprofile.php. The manipulation of the argument login_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-2025-1184	A vulnerability was found in pihome-shc PiHome 1.77 and classified as critical. Affected by this issue is some unknown functionality of the file /ajax.php?Ajax=GetModal_MQTTedit. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1201	A vulnerability was found in SourceCodester Best Church Management Software 1.1. It has been rated as critical. This issue affects some unknown processing of the file /admin/app/profile_crud.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.	6.3	More Details
CVE-2025-1197	A vulnerability has been found in code-projects Real Estate Property Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /_parse/load_user-profile.php. The manipulation of the argument userhash 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-2025-1199	A vulnerability was found in SourceCodester Best Church Management Software 1.1. It has been classified as critical. This affects an unknown part of the file /admin/app/role_crud.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1192	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been classified as critical. Affected is an unknown function of the file select-menu.php. The manipulation of the argument table leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1191	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0 and classified as critical. This issue affects some unknown processing of the file /dashboard/approve-reject.php. The manipulation of the argument breject_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1379	A vulnerability has been found in code-projects Real Estate Property Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Admin/CustomerReport.php. The manipulation of the argument city 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-2025-1189	A vulnerability, which was classified as critical, was found in 1000 Projects Attendance Tracking Management System 1.0. This affects an unknown part of the file /admin/chart1.php. The manipulation of the argument course_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-25204	`gh` is GitHub's official command line tool. Starting in version 2.49.0 and prior to version 2.67.0, under certain conditions, a bug in GitHub's Artifact Attestation cli tool `gh attestation verify` causes it to return a zero exit status when no attestations are present. This behavior is incorrect: When no attestations are present, `gh attestation verify` should return a non-zero exit status code, thereby signaling verification failure. An attacker can abuse this flaw to, for example, deploy malicious artifacts in any system that uses `gh attestation verify`'s exit codes to gatekeep deployments. Users are advised to update `gh` to patched version `v2.67.0` as soon as possible.	6.3	More Details
CVE-2025-1185	A vulnerability was found in pihome-shc PiHome 2.0. It has been classified as critical. This affects an unknown part of the file /ajax.php? Ajax=GetModal_Sensor_Graph. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1380	A vulnerability was found in Codezips Gym Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /dashboard/admin/del_plan.php. The manipulation of the argument name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1188	A vulnerability, which was classified as critical, has been found in Codezips Gym Management System 1.0. Affected by this issue is some unknown functionality of the file /dashboard/admin/updateroutine.php. The manipulation of the argument tid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1381	A vulnerability was found in code-projects Real Estate Property Management System 1.0. It has been classified as critical. This affects an unknown part of the file /ajax_city.php. The manipulation of the argument CityName leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-13689	The Uncode Core plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.9.1.6. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	6.3	More Details
CVE-2025-22702	Missing Authorization vulnerability in EPC Photography. This issue affects Photography: from n/a through 7.5.2.	6.3	More Details
CVE-2024-57603	An issue in MaysWind ezBookkeeping 0.7.0 allows a remote attacker to escalate privileges via the lack of rate limiting.	6.3	More Details
CVE-2025-1202	A vulnerability classified as critical has been found in SourceCodester Best Church Management Software 1.1. Affected is an unknown function of the file /admin/edit_slider.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1227	A vulnerability was found in ywoa up to 2024.07.03. It has been rated as critical. This issue affects the function selectList of the file com/cloudweb/oa/mapper/xml/AddressDao.xml. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1225	A vulnerability, which was classified as problematic, has been found in ywoa up to 2024.07.03. This issue affects the function extract of the file c-main/src/main/java/com/redmoon/weixin/aes/XMLParse.java of the component WXCallBack Interface. The manipulation leads to xml external entity reference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-1224	A vulnerability classified as critical was found in ywoa up to 2024.07.03. This vulnerability affects the function listNameBySql of the file com/cloudweb/oa/mapper/xml/UserMapper.xml. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-1216	A vulnerability, which was classified as critical, has been found in ywoa up to 2024.07.03. This issue affects the function selectNoticeList of the file com/cloudweb/oa/mapper/xml/OaNoticeMapper.xml. The manipulation of the argument sort leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-23411	mySCADA myPRO Manager is vulnerable to cross-site request forgery (CSRF), which could allow an attacker to obtain sensitive information. An attacker would need to trick the victim in to visiting an attacker-controlled website.	6.3	More Details
CVE-2025-1339	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329. It has been rated as critical. This issue affects the function setL2tpdConfig of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument enable leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-1210	A vulnerability classified as critical was found in code-projects Wazifa System 1.0. Affected by this vulnerability is an unknown functionality of the file /controllers/control.php. The manipulation of the argument to 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 Number	Description	Base Score	Reference
CVE-2025-1356	A vulnerability was found in needyamin Library Card System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file card.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-1206	A vulnerability was found in Codezips Gym Management System 1.0. It has been classified as critical. This affects an unknown part of the file /dashboard/admin/viewdetailroutine.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-1214	A vulnerability classified as critical has been found in pihome-shc PiHome 2.0. This affects an unknown part of the file /user_accounts.php?uid of the component Role-Based Access Control. The manipulation leads to missing authorization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-20615	The Qardio Arm iOS application exposes sensitive data such as usernames and passwords in a plist file. This allows an attacker to log in to production-level development accounts and access an engineering backdoor in the application. The engineering backdoor allows the attacker to send hex-based commands over a UI-based terminal.	6.2	More Details
CVE-2025-0426	A security issue was discovered in Kubernetes where a large number of container checkpoint requests made to the unauthenticated kubelet read-only HTTP endpoint may cause a Node Denial of Service by filling the Node's disk.	6.2	More Details
CVE-2024-11376	The s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 241114. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-1271	Reflected Cross-Site Scripting (XSS) in Anapi Group's h6web. This security flaw could allow an attacker to inject malicious JavaScript code into a URL. When a user accesses that URL, the injected code is executed in their browser, which can result in the theft of sensitive information, identity theft or the execution of unauthorised actions on behalf of the affected user.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13867	The Listivo - Classified Ads WordPress Theme theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in all versions up to, and including, 2.3.67 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-2024-13749	The StaffList plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.3. This is due to missing or incorrect nonce validation on the 'stafflist' 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-2025-25990	Cross Site Scripting vulnerability in hooskcms v.1.7.1 allows a remote attacker to obtain sensitive information via the /install/index.php component.	6.1	More Details
CVE-2024-41166	Stack-based buffer overflow in some Intel(R) PROSet/Wireless WiFi and Killerâ„¢ WiFi software for Windows before version 23.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.1	More Details
CVE-2025-0864	The Active Products Tables for WooCommerce. Use constructor to create tables plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shortcodes_set' parameter in all versions up to, and including, 1.0.6.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-25296	Label Studio is an open source data labeling tool. Prior to version 1.16.0, Label Studio's `/projects/upload-example` endpoint allows injection of arbitrary HTML through a `GET` request with an appropriately crafted `label_config` query parameter. By crafting a specially formatted XML label config with inline task data containing malicious HTML/JavaScript, an attacker can achieve Cross-Site Scripting (XSS). While the application has a Content Security Policy (CSP), it is only set in report-only mode, making it ineffective at preventing script execution. The vulnerability exists because the upload-example endpoint renders user-provided HTML content without proper sanitization on a GET request. This allows attackers to inject and execute arbitrary JavaScript in victims' browsers by getting them to visit a maliciously crafted URL. This is considered vulnerable because it enables attackers to execute JavaScript in victims' contexts, potentially allowing theft of sensitive data, session hijacking, or other malicious actions. Version 1.16.0 contains a patch for the issue.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13522	The magayo Lottery Results plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.12. This is due to missing or incorrect nonce validation on the 'magayo-lottery-results' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-40887	Race condition in some Intel(R) PROSet/Wireless WiFi and Killerâ„¢ WiFi software for Windows before version 23.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.1	More Details
CVE-2023-32277	Untrusted Pointer Dereference in I/O subsystem for some Intel(R) QAT software before version 2.0.5 may allow authenticated user to potentially enable information disclosure via local operating system access.	6.1	More Details
CVE-2024-39606	Improper input validation in some Intel(R) PROSet/Wireless WiFi and Killerâ„¢ WiFi software for Windows before version 23.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.1	More Details
CVE-2024-13523	The MemorialDay plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.4. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-1390	The PAM module pam_cap.so of libcap configuration supports group names starting with “@”, during actual parsing, configurations not starting with “@” are incorrectly recognized as group names. This may result in nonintended users being granted an inherited capability set, potentially leading to security risks. Attackers can exploit this vulnerability to achieve local privilege escalation on systems where /etc/security/capability.conf is used to configure user inherited privileges by constructing specific usernames.	6.1	More Details
CVE-2024-30211	Improper access control in some Intel(R) ME driver pack installer engines before version 2422.6.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.0	More Details
CVE-2024-41934	Improper access control in some Intel(R) GPA software before version 2024.3 may allow an authenticated user to potentially enable denial of service via local access.	5.9	More Details
CVE-2025-26778	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Gallery allows Stored XSS. This issue affects Gallery: from n/a through 2.2.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29171	Dell BSAFE SSL-J, versions prior to 6.6 and versions 7.0 through 7.2, contains an Improper certificate verification vulnerability. A remote attacker could potentially exploit this vulnerability, leading to information disclosure.	5.9	More Details
CVE-2024-29172	Dell BSAFE SSL-J, versions prior to 6.6 and versions 7.0 through 7.2, contains a deadlock vulnerability. A remote attacker could potentially exploit this vulnerability, leading to a Denial of Service.	5.9	More Details
CVE-2025-26775	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 BEAR allows Stored XSS. This issue affects BEAR: from n/a through 1.1.4.4.	5.9	More Details
CVE-2024-13641	The Return Refund and Exchange For WooCommerce – Return Management System, RMA Exchange, Wallet And Cancel Order Features plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.4.5 via the 'attachment' directory. This makes it possible for unauthenticated attackers to extract sensitive data stored insecurely in the /wp-content/attachment directory which can contain file attachments for order refunds.	5.9	More Details
CVE-2024-13609	The 1 Click WordPress Migration Plugin – 100% FREE for a limited time plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.1 via the class-ocm-backup.php. This makes it possible for unauthenticated attackers to extract sensitive data including usernames and their respective password hashes during a short window of time in which the backup is in process.	5.9	More Details
CVE-2025-26561	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in elfsight Elfsight Yottie Lite allows Stored XSS. This issue affects Elfsight Yottie Lite: from n/a through 1.3.3.	5.9	More Details
CVE-2025-0997	Use after free in Navigation in Google Chrome prior to 133.0.6943.98 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	5.9	More Details
CVE-2025-26157	A SQL Injection vulnerability was found in /bpms/index.php in Source Code and Project Beauty Parlour Management System V1.1, which allows remote attackers to execute arbitrary code via the name POST request parameter.	5.9	More Details
CVE-2025-0998	Out of bounds memory access in V8 in Google Chrome prior to 133.0.6943.98 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	5.9	More Details
CVE-2025-0995	Use after free in V8 in Google Chrome prior to 133.0.6943.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0996	Inappropriate implementation in Browser UI in Google Chrome on Android prior to 133.0.6943.98 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	5.9	More Details
CVE-2025-24607	Missing Authorization vulnerability in Northern Beaches Websites IdeaPush allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects IdeaPush: from n/a through 8.71.	5.8	More Details
CVE-2024-12012	A CWE-598 "Use of GET Request Method with Sensitive Query Strings" was discovered affecting the 130.8005 TCP/IP Gateway running firmware version 12h. Both the SHA-1 hash of the password as well as the session tokens are included as part of the URL and therefore exposed to information leakage scenarios. An attacker capable of accessing such values (e.g., victim browser, network traffic inspection) can exploit this vulnerability to leak both the password hash as well as session tokens and bypass the authentication mechanism using a pass-the-hash attack.	5.7	More Details
CVE-2025-1035	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Komtera Technologies KLog Server allows Manipulating Web Input to File System Calls.This issue affects KLog Server: before 3.1.1.	5.7	More Details
CVE-2025-26158	A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the manage-employee.php page of Kashipara Online Attendance Management System V1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the department parameter.	5.6	More Details
CVE-2024-36285	Race condition in some Intel(R) PROSet/Wireless WiFi and Killerâ„¢ WiFi software for Windows before version 23.80 may allow an authenticated user to potentially enable denial of service via local access.	5.6	More Details
CVE-2024-13879	The Stream plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.0.2 due to insufficient validation on the webhook feature. 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 which can be used to query and modify information from internal services.	5.5	More Details
CVE-2025-21699	In the Linux kernel, the following vulnerability has been resolved: gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1102	A CWE-346 "Origin Validation Error" in the CORS configuration in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to affect the device confidentiality, integrity, or availability via crafted URLs or HTTP requests.	5.5	More Details
CVE-2024-13848	The Reaction Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2024-21971	Improper input validation in AMD Crash Defender could allow an attacker to provide the Windows® system process ID to a kernel-mode driver, resulting in an operating system crash, potentially leading to denial of service.	5.5	More Details
CVE-2025-26358	A CWE-20 "Improper Input Validation" in ldbMT.so in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to modify system configuration via crafted HTTP requests.	5.5	More Details
CVE-2024-57952	In the Linux kernel, the following vulnerability has been resolved: Revert "libfs: fix infinite directory reads for offset dir" The current directory offset allocator (based on mtree_alloc_cyclic) stores the next offset value to return in octx->next_offset. This mechanism typically returns values that increase monotonically over time. Eventually, though, the newly allocated offset value wraps back to a low number (say, 2) which is smaller than other already- allocated offset values. Yu Kuai <yukuai3@huawei.com> reports that, after commit 64a7ce76fb90 ("libfs: fix infinite directory reads for offset dir"), if a directory's offset allocator wraps, existing entries are no longer visible via readdir/getdents because offset_readdir() stops listing entries once an entry's offset is larger than octx->next_offset. These entries vanish persistently -- they can be looked up, but will never again appear in readdir(3) output. The reason for this is that the commit treats directory offsets as monotonically increasing integer values rather than opaque cookies, and introduces this comparison: if (dentry2offset(dentry) >= last_index) { On 64-bit platforms, the directory offset value upper bound is 2^63 - 1. Directory offsets will monotonically increase for millions of years without wrapping. On 32-bit platforms, however, LONG_MAX is 2^31 - 1. The allocator can wrap after only a few weeks (at worst). Revert commit 64a7ce76fb90 ("libfs: fix infinite directory reads for offset dir") to prepare for a fix that can work properly on 32-bit systems and might apply to recent LTS kernels where shmem employs the simple_offset mechanism.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-21696	In the Linux kernel, the following vulnerability has been resolved: mm: clear uffd-wp PTE/PMD state on mremap() When mremap()ing a memory region previously registered with userfaultfd as write-protected but without UFFD_FEATURE_EVENT_REMAP, an inconsistency in flag clearing leads to a mismatch between the vma flags (which have uffd-wp cleared) and the pte/pmd flags (which do not have uffd-wp cleared). This mismatch causes a subsequent mprotect(PROT_WRITE) to trigger a warning in page_table_check_pte_flags() due to setting the pte to writable while uffd-wp is still set. Fix this by always explicitly clearing the uffd-wp pte/pmd flags on any such mremap() so that the values are consistent with the existing clearing of VM_UFFD_WP. Be careful to clear the logical flag regardless of its physical form; a PTE bit, a swap PTE bit, or a PTE marker. Cover PTE, huge PMD and hugetlb paths.	5.5	More Details
CVE-2025-26348	A CWE-89 "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')" in maxprofile/menu/model.lua (editUserMenu endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to execute arbitrary SQL commands via crafted HTTP requests.	5.5	More Details
CVE-2024-10083	CWE-20: Improper Input Validation vulnerability exists that could cause denial of service of engineering workstation when specific driver interface is invoked locally by an authenticated user with crafted input.	5.5	More Details
CVE-2024-10404	CallInvocationHandler in Brocade SANnav before 2.3.1b logs sensitive information in clear text. The vulnerability could allow an authenticated, local attacker to view Brocade Fabric OS switch sensitive information in clear text. An attacker with administrative privileges could retrieve sensitive information including passwords; SNMP responses that contain AuthSecret and PrivSecret after collecting a "supportsave" or getting access to an already collected "supportsave". NOTE: this issue exists because of an incomplete fix for CVE-2024-29952	5.5	More Details
CVE-2025-21697	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Ensure job pointer is set to NULL after job completion After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading the driver, as it appears the job is still active. To prevent this, assign the job pointer to NULL after completing the job, indicating the job has finished.	5.5	More Details
CVE-2025-26346	A CWE-89 "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')" in maxprofile/menu/model.lua (editUserGroupMenu endpoint) in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to execute arbitrary SQL commands via crafted HTTP requests.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-21694	In the Linux kernel, the following vulnerability has been resolved: fs/proc: fix softlockup in __read_vmcore (part 2) Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes. In a memory constrained environment like the kdump image, a softlockup is not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck. The second loop in __read_vmcore has a lot more opportunities for natural sleep points, like scheduling out while waiting for a data write to happen, but apparently that is not always enough. Add a cond_resched() to the second loop in __read_vmcore to (hopefully) get rid of the softlockups.	5.5	More Details
CVE-2024-13814	The The Global Gallery - WordPress Responsive Gallery plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 9.1.5. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	5.4	More Details
CVE-2024-13667	The Uncode theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mle-description' parameter in all versions up to, and including, 2.9.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-13741	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to Limited Server-Side Request Forgery in all versions up to, and including, 5.9.4.2 via the pm_upload_image function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to download and view images, as well as validating if a non-image file exists, both on local or remote hosts.	5.4	More Details
CVE-2024-56938	LearnDash v6.7.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the materials-content class.	5.4	More Details
CVE-2024-12054	ZF Roll Stability Support Plus (RSSPlus) is vulnerable to an authentication bypass vulnerability targeting deterministic RSSPlus SecurityAccess service seeds, which may allow an attacker to remotely (proximal/adjacent with RF equipment or via pivot from J2497 telematics devices) call diagnostic functions intended for workshop or repair scenarios. This can impact system availability, potentially degrading performance or erasing software, however the vehicle remains in a safe vehicle state.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-57056	Incorrect cookie session handling in WombatDialer before 25.02 results in the full session identity being written to system logs and could be used by a malicious attacker to impersonate an existing user session.	5.4	More Details
CVE-2024-54951	Monica 4.1.2 is vulnerable to Cross Site Scripting (XSS). A malicious user can create a malformed contact and use that contact in the "HOW YOU MET" customization options to trigger the XSS.	5.4	More Details
CVE-2025-1391	A flaw was found in the Keycloak organization feature, which allows the incorrect assignment of an organization to a user if their username or email matches the organization's domain pattern. This issue occurs at the mapper level, leading to misrepresentation in tokens. If an application relies on these claims for authorization, it may incorrectly assume a user belongs to an organization they are not a member of, potentially granting unauthorized access or privileges.	5.4	More Details
CVE-2024-13692	The Return Refund and Exchange For WooCommerce – Return Management System, RMA Exchange, Wallet And Cancel Order Features plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.4.5 via several functions due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to overwrite linked refund image attachments, overwrite refund request message, overwrite order messages, and read order messages of other users.	5.4	More Details
CVE-2025-26765	Missing Authorization vulnerability in enituretechnology Distance Based Shipping Calculator allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Distance Based Shipping Calculator: from n/a through 2.0.22.	5.4	More Details
CVE-2024-56939	LearnDash v6.7.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Id-comment-body class.	5.4	More Details
CVE-2024-13834	The Responsive Plus – Starter Templates, Advanced Features and Customizer Settings for Responsive Theme plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.1.4 via the 'remote_request' function. This makes it possible for authenticated attackers, with contributor-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.	5.4	More Details
CVE-2024-31068	Improper Finite State Machines (FSMs) in Hardware Logic for some Intel(R) Processors may allow privileged user to potentially enable denial of service via local access.	5.3	More Details
CVE-2024-31157	Improper initialization in UEFI firmware OutOfBandXML module in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13555	The 1 Click WordPress Migration Plugin – 100% FREE for a limited time plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1. This is due to missing or incorrect nonce validation on the cancel_actions() function. This makes it possible for unauthenticated attackers to cancel a triggered backup via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2024-13538	The BigBuy Dropshipping Connector for WooCommerce plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.9.19. This is due the /vendor/cocur/sluggify/bin/generate-default.php file being directly accessible and triggering an error. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-13540	The WooODT Lite – Delivery & pickup date time location for WooCommerce plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.5.1. This is due the /inc/bycwooodt_get_all_orders.php file being publicly accessible and generating a publicly visible error message. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2025-1101	A CWE-204 "Observable Response Discrepancy" in the login page in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to enumerate valid usernames via crafted HTTP requests.	5.3	More Details
CVE-2025-26360	A CWE-306 "Missing Authentication for Critical Function" in maxprofile/persistence/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an unauthenticated remote attacker to delete dashboards via crafted HTTP requests.	5.3	More Details
CVE-2024-28047	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2025-1372	A vulnerability was found in GNU elfutils 0.192. It has been declared as critical. Affected by this vulnerability is the function dump_data_section/print_string_section of the file readelf.c of the component eu-readelf. The manipulation of the argument z/x leads to buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of the patch is 73db9d2021cab9e23fd734b0a76a612d52a6f1db. It is recommended to apply a patch to fix this issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21859	Improper buffer restrictions in the UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2023-48366	Race condition in some Intel(R) System Security Report and System Resources Defense firmware may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2025-1226	A vulnerability was found in ywoa up to 2024.07.03. It has been declared as critical. This vulnerability affects unknown code of the file /oa/setup/setup.jsp. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2025-22645	Improper Restriction of Excessive Authentication Attempts vulnerability in Rameez Iqbal Real Estate Manager allows Password Brute Forcing. This issue affects Real Estate Manager: from n/a through 7.3.	5.3	More Details
CVE-2025-1370	A vulnerability, which was classified as critical, has been found in MicroWorld eScan Antivirus 7.0.32 on Linux. Affected by this issue is the function sprintf of the file epsdaemon of the component Autoscan USB. The manipulation leads to os command injection. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-6097	In Progress® Telerik® Reporting versions prior to 2025 Q1 (19.0.25.211), information disclosure is possible by a local threat actor through an absolute path vulnerability.	5.3	More Details
CVE-2025-27013	Missing Authorization vulnerability in EPC MediCenter - Health Medical Clinic WordPress Theme allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MediCenter - Health Medical Clinic WordPress Theme: from n/a through n/a.	5.3	More Details
CVE-2025-1367	A vulnerability was found in MicroWord eScan Antivirus 7.0.32 on Linux. It has been classified as critical. This affects the function sprintf of the component USB Password Handler. The manipulation leads to buffer overflow. An attack has to be approached locally. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1366	A vulnerability was found in MicroWord eScan Antivirus 7.0.32 on Linux and classified as critical. Affected by this issue is the function strcpy of the component VirusPopUp. The manipulation leads to stack-based buffer overflow. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-1365	A vulnerability, which was classified as critical, was found in GNU elfutils 0.192. This affects the function process_symtab of the file readelf.c of the component eu-readelf. The manipulation of the argument D/a leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of the patch is 5e5c0394d82c53e97750fe7b18023e6f84157b81. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-1364	A vulnerability has been found in MicroWord eScan Antivirus 7.0.32 on Linux and classified as critical. Affected by this vulnerability is the function passPrompt of the component USB Protection Service. The manipulation leads to stack-based buffer overflow. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-22291	Missing Authorization vulnerability in enituretechnology LTL Freight Quotes – Worldwide Express Edition allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects LTL Freight Quotes – Worldwide Express Edition: from n/a through 5.0.20.	5.3	More Details
CVE-2025-1187	A vulnerability classified as critical was found in code-projects Police FIR Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the component Delete Record Handler. The manipulation leads to stack-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-13535	The Actionwear products sync plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.3.0. This is due the composer-setup.php file being publicly accessible with 'display_errors' set to true. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13821	The WP Booking Calendar plugin for WordPress is vulnerable to Unauthenticated Post-Confirmation Booking Manipulation in all versions up to, and including, 10.10. This is due to the plugin not properly requiring re-verification after a booking has been made and a change is being attempted. This makes it possible for unauthenticated attackers to manipulate their confirmed bookings, even after they have been approved.	5.3	More Details
CVE-2024-13316	The Scratch & Win – Giveaways and Contests. Boost subscribers, traffic, repeat visits, referrals, sales and more plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the apmswn_create_discount() function in all versions up to, and including, 2.8.0. This makes it possible for unauthenticated attackers to create coupons.	5.3	More Details
CVE-2025-0814	CWE-20: Improper Input Validation vulnerability exists that could cause Denial-of-Service of the network services running on the product when malicious IEC61850-MMS packets are sent to the device. The core functionality of the breaker remains intact during the attack.	5.3	More Details
CVE-2025-25290	@octokit/request sends parameterized requests to GitHub's APIs with sensible defaults in browsers and Node. Starting in version 1.0.0 and prior to version 9.2.1, the regular expression `/<([>]+)>; rel="deprecation"/` used to match the `link` header in HTTP responses is vulnerable to a ReDoS (Regular Expression Denial of Service) attack. This vulnerability arises due to the unbounded nature of the regex's matching behavior, which can lead to catastrophic backtracking when processing specially crafted input. An attacker could exploit this flaw by sending a malicious `link` header, resulting in excessive CPU usage and potentially causing the server to become unresponsive, impacting service availability. Version 9.2.1 fixes the issue.	5.3	More Details
CVE-2025-25289	@octokit/request-error is an error class for Octokit request errors. Starting in version 1.0.0 and prior to version 6.1.7, a Regular Expression Denial of Service (ReDoS) vulnerability exists in the processing of HTTP request headers. By sending an authorization header containing an excessively long sequence of spaces followed by a newline and "@", an attacker can exploit inefficient regular expression processing, leading to excessive resource consumption. This can significantly degrade server performance or cause a denial-of-service (DoS) condition, impacting availability. Version 6.1.7 contains a fix for the issue.	5.3	More Details
CVE-2025-25288	@octokit/plugin-paginate-rest is the Octokit plugin to paginate REST API endpoint responses. For versions starting in 1.0.0 and prior to 11.4.1 of the npm package `@octokit/plugin-paginate-rest`, when calling `octokit.paginate.iterator()`, a specially crafted `octokit` instance—particularly with a malicious `link` parameter in the `headers` section of the `request`—can trigger a ReDoS attack. Version 11.4.1 contains a fix for the issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13554	The The Ultimate WordPress Toolkit – WP Extended plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the <code>reorder_route()</code> function in all versions up to, and including, 3.0.13. This makes it possible for unauthenticated attackers to reorder posts.	5.3	More Details
CVE-2025-25285	@octokit/endpoint turns REST API endpoints into generic request options. Starting in version 4.1.0 and prior to version 10.1.3, by crafting specific <code>`options`</code> parameters, the <code>`endpoint.parse(options)`</code> call can be triggered, leading to a regular expression denial-of-service (ReDoS) attack. This causes the program to hang and results in high CPU utilization. The issue occurs in the <code>`parse`</code> function within the <code>`parse.ts`</code> file of the npm package <code>`@octokit/endpoint`</code> . Version 10.1.3 contains a patch for the issue.	5.3	More Details
CVE-2025-26758	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in RebelCode Spotlight Social Media Feeds allows Retrieve Embedded Sensitive Data. This issue affects Spotlight Social Media Feeds: from n/a through 1.7.1.	5.3	More Details
CVE-2024-13539	The AForms Eats plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.3.1. This is due the <code>/vendor/aura/payload-interface/phpunit.php</code> file being publicly accessible and displaying error messages. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-13794	The WP Ghost (Hide My WP Ghost) – Security & Firewall plugin for WordPress is vulnerable to Login Page Disclosure in all versions up to, and including, 5.3.02. This is due to the plugin not properly restricting the <code>/wp-register.php</code> path. This makes it possible for unauthenticated attackers to discover the hidden login page location.	5.3	More Details
CVE-2024-45775	A flaw was found in grub2 where the <code>grub_extcmd_dispatcher()</code> function calls <code>grub_arg_list_alloc()</code> to allocate memory for the grub's argument list. However, it fails to check in case the memory allocation fails. Once the allocation fails, a NULL point will be processed by the <code>parse_option()</code> function, leading grub to crash or, in some rare scenarios, corrupt the IVT data.	5.2	More Details
CVE-2025-25991	SQL Injection vulnerability in hooskcms v.1.7.1 allows a remote attacker to obtain sensitive information via the <code>/install/index.php</code> component.	5.1	More Details
CVE-2025-25993	SQL Injection vulnerability in FeMiner wms wms 1.0 allows a remote attacker to obtain sensitive information via the parameter "itemid."	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25992	SQL Injection vulnerability in FeMiner wms 1.0 allows a remote attacker to obtain sensitive information via the inquire_inout_item.php component.	5.1	More Details
CVE-2025-1352	A vulnerability has been found in GNU elfutils 0.192 and classified as critical. This vulnerability affects the function __libdw_thread_tail in the library libdw_alloc.c of the component eu-readelf. The manipulation of the argument w leads to memory corruption. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The name of the patch is 2636426a091bd6c6f7f02e49ab20d4cdc6bfc753. It is recommended to apply a patch to fix this issue.	5.0	More Details
CVE-2024-31153	Improper input validation for some Intel(R) QuickAssist Technology software before version 2.2.0 may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2023-20508	Improper access control in the ASP could allow a privileged attacker to perform an out-of-bounds write to a memory location not controlled by the attacker, potentially leading to loss of confidentiality, integrity, or availability.	5.0	More Details
CVE-2024-53880	NVIDIA Triton Inference Server contains a vulnerability in the model loading API, where a user could cause an integer overflow or wraparound error by loading a model with an extra-large file size that overflows an internal variable. A successful exploit of this vulnerability might lead to denial of service.	4.9	More Details
CVE-2025-26350	A CWE-434 "Unrestricted Upload of File with Dangerous Type" in the template file uploads in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to upload malicious files via crafted HTTP requests.	4.9	More Details
CVE-2025-25900	A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11 via the username and password parameters at /userRpm/PPPoEv6CfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	4.9	More Details
CVE-2025-26351	A CWE-35 "Path Traversal" in the template download mechanism in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to read sensitive files via crafted HTTP requests.	4.9	More Details
CVE-2025-26353	A CWE-35 "Path Traversal" in maxtime/api/sql/sql.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to read sensitive files via crafted HTTP requests.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26357	A CWE-35 "Path Traversal" in maxtime/api/database/database.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated remote attacker to read sensitive files via crafted HTTP requests.	4.9	More Details
CVE-2024-13791	Bit Assist plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.2 via the downloadResponseFile() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2025-26779	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Fahad Mahmood Keep Backup Daily allows Path Traversal. This issue affects Keep Backup Daily: from n/a through 2.1.0.	4.9	More Details
CVE-2025-1042	An insecure direct object reference vulnerability in GitLab EE affecting all versions from 15.7 prior to 17.6.5, 17.7 prior to 17.7.4, and 17.8 prior to 17.8.2 allows an attacker to view repositories in an unauthorized way.	4.9	More Details
CVE-2024-47264	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in agent-related functionality in Synology Active Backup for Business before 2.7.1-13234, 2.7.1-23234 and 2.7.1-3234 allows remote authenticated users with administrator privileges to delete arbitrary files via unspecified vectors.	4.9	More Details
CVE-2025-1269	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in HAVELSAN Liman MYS allows Cross-Site Flashing.This issue affects Liman MYS: before 2.1.1 - 1010.	4.8	More Details
CVE-2025-1230	Stored Cross-Site Scripting (XSS) vulnerability in Prestashop 8.1.7, due to the lack of proper validation of user input through '/<admin_directory>/index.php', affecting the 'link' parameter. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	4.8	More Details
CVE-2024-7052	The Forminator Forms WordPress plugin before 1.38.3 does not sanitise and escape some of its settings, which could allow high privilege users such as Admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-13493	The Sensly Online Presence WordPress plugin through 0.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13119	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content WordPress plugin before 4.15.20 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-56463	IBM QRadar SIEM 7.5 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2025-25988	Cross Site Scripting vulnerability in hooskcms v.1.8 allows a remote attacker to cause a denial of service via the custom Link title parameter and the Title parameter.	4.8	More Details
CVE-2025-22209	A SQL injection vulnerability in the JS Jobs plugin versions 1.1.5-1.4.3 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands via the 'searchpaymentstatus' parameter in the Employer Payment History search feature.	4.7	More Details
CVE-2025-25287	Lakeus is a simple skin made for MediaWiki. Starting in version 1.8.0 and prior to versions 1.3.1+REL1.39, 1.3.1+REL1.42, and 1.4.0, Lakeus is vulnerable to store cross-site scripting via malicious system messages, though editing the messages requires high privileges. Those with `(editinterface)` rights can edit system messages that are improperly handled in order to send raw HTML. In the case of `lakeus-footermessag`, this will affect all users if the server is configured to link back to this repository. Otherwise, the system messages in themeDesigner.js are only used when the user enables it in their preferences. Versions 1.3.1+REL1.39, 1.3.1+REL1.42, and 1.4.0 contain a patch.	4.7	More Details
CVE-2022-28693	Unprotected alternative channel of return branch target prediction in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	4.7	More Details
CVE-2025-22208	A SQL injection vulnerability in the JS Jobs plugin versions 1.1.5-1.4.3 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands via the 'filter_email' parameter in the GDPR Erase Data Request search feature.	4.7	More Details
CVE-2024-39779	Stack-based buffer overflow in some drivers for Intel(R) Ethernet Connection I219 Series before version 12.19.1.39 may allow an authenticated user to potentially enable denial of service via local access.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-21695	In the Linux kernel, the following vulnerability has been resolved: platform/x86: dell-uart-backlight: fix serdev race The dell_uart_bl_serdev_probe() function calls devm_serdev_device_open() before setting the client ops via serdev_device_set_client_ops(). This ordering can trigger a NULL pointer dereference in the serdev controller's receive_buf handler, as it assumes serdev->ops is valid when SERPORT_ACTIVE is set. This is similar to the issue fixed in commit 5e700b384ec1 ("platform/chrome: cros_ec_uart: properly fix race condition") where devm_serdev_device_open() was called before fully initializing the device. Fix the race by ensuring client ops are set before enabling the port via devm_serdev_device_open(). Note, serdev_device_set_baudrate() and serdev_device_set_flow_control() calls should be after the devm_serdev_device_open() call.	4.7	More Details
CVE-2024-37601	An issue was discovered in Mercedes Benz NTG (New Telematics Generation) 6. A possible heap buffer overflow exists in the user data import/export function of NTG 6 head units. To perform this attack, local access to the USB interface of the car is needed. With prepared data, an attacker can cause the User-Data service to fail. The failed service instance will restart automatically.	4.6	More Details
CVE-2024-37602	An issue was discovered in Mercedes Benz NTG (New Telematics Generation) 6 through 2021. A possible NULL pointer dereference in the Apple Car Play function affects NTG 6 head units. To perform this attack, physical access to Ethernet pins of the head unit base board is needed. With a static IP address, an attacker can connect via the internal network to the iTunes / AirPlay service. With prepared HTTP requests, an attacker can cause the Car Play service to fail.	4.6	More Details
CVE-2024-37603	An issue was discovered in Mercedes Benz NTG (New Telematics Generation) 6. A possible type confusion exists in the user data import/export function of NTG 6 head units. To perform this attack, local access to the USB interface of the car is needed. With prepared data, an attacker can cause the User-Data service to fail. The failed service instance will restart automatically.	4.6	More Details
CVE-2025-1369	A vulnerability classified as critical was found in MicroWord eScan Antivirus 7.0.32 on Linux. Affected by this vulnerability is an unknown functionality of the component USB Password Handler. The manipulation leads to os command injection. The attack needs to be approached locally. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-24889	The SecureDrop Client is a desktop application for journalists to communicate with sources and work with submissions on the SecureDrop Workstation. Prior to versions 0.14.1 and 1.0.1, an attacker who has already gained code execution in a virtual machine on the SecureDrop Workstation could gain code execution in the `sd-log` virtual machine by sending a specially crafted log entry. The vulnerability is not exploitable remotely and requires an attacker to already have code execution on one of the other virtual machines (VMs) of the system. Due to the Workstation's underlying usage of Qubes for strong isolation, the vulnerability would have allowed lateral movement between any log-enabled VM and the `sd-log` VM, but no further. The SecureDrop workstation collects logs centrally in an isolated virtual machine named `sd-log` for easy export for support and debugging purposes. The `sd-log` VM is completely isolated from the internet and ingests logs via a narrow Qubes RPC policy that allows for specific inter-VM communication via the Xen vchan protocol used by Qubes's qrexec mechanism. A path traversal bug was found in the logic used to choose where to write the log file for a specific VM: the VM name, used unsanitized in the destination path in `sd-log`, is supplied by the logging VM itself instead of being read from a trusted source, such as the Qubes environment variable `QREXEC_REMOTE_DOMAIN` that is used in the fixed implementation. An attacker could provide an arbitrary source VM name, possibly overwriting logs of other VMs, or writing a file named `syslog.log`, with attacker-controlled content, in arbitrary directories as a low-privileged user. A successful attack could potentially overwrite or add configuration to software that loads configuration files from a directory. This is exploitable to achieve code execution by setting the target directory to `/home/user/.config/autostart/` and letting it write `syslog.log`, because XFCE treats any file in that directory as a `.desktop` file regardless of its extension. Versions 0.14.1 and 1.0.1 contain a patch for this issue.	4.5	More Details
CVE-2025-26791	DOMPurify before 3.2.4 has an incorrect template literal regular expression, sometimes leading to mutation cross-site scripting (mXSS).	4.5	More Details
CVE-2025-21401	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	4.5	More Details
CVE-2024-45783	A flaw was found in grub2. When failing to mount an HFS+ grub, the hfsplus filesystem driver doesn't properly set an ERRNO value. This issue may lead to a NULL pointer access.	4.4	More Details
CVE-2024-8266	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.1 prior to 17.6.0, which allows an attacker with maintainer role to trigger a pipeline as project owner under certain circumstances.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13437	The Book a Room plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.9. This is due to missing or incorrect nonce validation on the 'bookaroom_Settings' page. This makes it possible for unauthenticated attackers to update 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.	4.3	More Details
CVE-2024-13541	The aDirectory – WordPress Directory Listing Plugin plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the adqs_delete_listing() function in all versions up to, and including, 2.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary posts.	4.3	More Details
CVE-2024-25066	RSA Authentication Manager before 8.7 SP2 Patch 1 allows XML External Entity (XXE) attacks via a license file, resulting in attacker-controlled files being stored on the product's server. Data exfiltration cannot occur.	4.3	More Details
CVE-2025-0808	The Houzez Property Feed plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.4.21. This is due to missing or incorrect nonce validation on the "deleteexport" action. This makes it possible for unauthenticated attackers to delete property feed exports via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-13374	The WP Table Manager plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on thewptm_getFolders AJAX action in all versions up to, and including, 4.1.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary file names and directories.	4.3	More Details
CVE-2024-12164	The WPSyncSheets Lite For WPForms – WPForms Google Spreadsheet Addon plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpsslwp_reset_settings() function in all versions up to, and including, 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-2024-13740	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.9.4.2 via the pm_messenger_show_messages function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read private conversations of other users.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26773	Missing Authorization vulnerability in Adnan Analytify allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Analytify: from n/a through 5.5.0.	4.3	More Details
CVE-2024-13601	The Majestic Support - The Leading-Edge Help Desk & Customer Support Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.0.5 via the 'exportusereraserequest' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export ticket data for any user.	4.3	More Details
CVE-2024-13687	The Team Builder - Meet the Team plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_team_builder_options() function in all versions up to, and including, 1.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings.	4.3	More Details
CVE-2025-26367	A CWE-862 "Missing Authorization" in maxprofile/user-groups/routes.lua in Q-Free MaxTime less than or equal to version 2.11.0 allows an authenticated (low-privileged) attacker to create arbitrary user groups via crafted HTTP requests.	4.3	More Details
CVE-2024-13439	The Team - Team Members Showcase Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the response() function in all versions up to, and including, 4.4.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings.	4.3	More Details
CVE-2025-0935	The Media Library Folders plugin for WordPress is vulnerable to unauthorized plugin settings change due to a missing capability check on several AJAX actions in all versions up to, and including, 8.3.0. This makes it possible for authenticated attackers, with Author-level access and above, to change plugin settings related to things such as IP-blocking.	4.3	More Details
CVE-2024-13306	The Maps Plugin using Google Maps for WordPress WordPress plugin before 1.9.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.3	More Details
CVE-2025-1212	An information disclosure vulnerability in GitLab CE/EE affecting all versions from 8.3 prior to 17.6.5, 17.7 prior to 17.7.4, and 17.8 prior to 17.8.2 allows an attacker to send a crafted request to a backend server to reveal sensitive information.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13208	The Maps Plugin using Google Maps for WordPress WordPress plugin before 1.9.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.3	More Details
CVE-2025-1228	A vulnerability classified as problematic has been found in olajowon Loggrove up to e428fac38cc480f011afcb1d8ce6c2bad378ddd6. Affected is an unknown function of the file /read/?page=1&logfile=LOG_Monitor of the component Logfile Update Handler. The manipulation of the argument path leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	4.3	More Details
CVE-2025-20097	Uncaught exception in OpenBMC Firmware for the Intel(R) Server M50FCP Family and Intel(R) Server D50DNP Family before version R01.02.0002 may allow an authenticated user to potentially enable denial of service via network access.	4.3	More Details
CVE-2024-13229	The Rank Math SEO - AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the update_metadata() function in all versions up to, and including, 1.0.235. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete any schema metadata assigned to any post.	4.3	More Details
CVE-2024-13783	The FormCraft plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check in formcraft-main.php in all versions up to, and including, 3.9.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export all plugin data which may contain sensitive information from form submissions.	4.3	More Details
CVE-2025-0661	The DethemeKit For Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.36 via the duplicate_post() function due to insufficient restrictions on which posts can be duplicated. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from password protected, private, draft, or scheduled posts that they should not have access to by duplicating the post.	4.3	More Details
CVE-2024-13639	The Read More & Accordion plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the expmDeleteData() function in all versions up to, and including, 3.4.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary 'read more' posts.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-13718	The Flexible Wishlist for WooCommerce – Ecommerce Wishlist & Save for later plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.26. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to modify/update/create other user's wishlists via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-25195	Zulip is an open source team chat application. A weekly cron job (added in 50256f48314250978f521ef439cafa704e056539) demotes channels to being "inactive" after they have not received traffic for 180 days. However, upon doing so, an event was sent to all users in the organization, not just users in the channel. This event contained the name of the private channel. Similarly, the same commit (50256f48314250978f521ef439cafa704e056539) added functionality to notify clients when channels stopped being "inactive." The first message sent to a private channel which had not previously had any messages for over 180 days (and were thus already marked "inactive") would leak an event to all users in the organization; this event also contained the name of the private channel. Commits 75be449d456d29fef27e9d1828bafa30174284b4 and a2a1a7f8d152296c8966f1380872c0ac69e5c87e fixed the issue. This vulnerability only existed in `main`, and was not part of any published versions.	4.3	More Details
CVE-2024-13795	The Ecwid by Lightspeed Ecommerce Shopping Cart plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.12.27. This is due to missing or incorrect nonce validation on the ecwid_deactivate_feedback() function. This makes it possible for unauthenticated attackers to send deactivation messages on behalf of a site owner via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-13438	The SpeedSize Image & Video AI-Optimizer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.1. This is due to missing or incorrect nonce validation on the 'speedsize_clear_css_cache_action' function. This makes it possible for unauthenticated attackers to clear the plugins cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-0796	The Mortgage Lead Capture System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 8.2.10. This is due to missing or incorrect nonce validation on the 'wprequal_reset_defaults' action. This makes it possible for unauthenticated attackers to reset the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10581	The DirectoryPress Frontend plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.9. This is due to missing or incorrect nonce validation on the dpfl_listingStatusChange() function. This makes it possible for unauthenticated attackers to update listing statuses via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-57969	app/Model/Attribute.php in MISP before 2.4.198 ignores an ACL during a GUI attribute search.	4.3	More Details
CVE-2025-1335	A vulnerability, which was classified as problematic, was found in CmsEasy 7.7.7.9. Affected is the function deleteimg_action in the library lib/admin/file_admin.php. The manipulation of the argument imgname leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-1336	A vulnerability has been found in CmsEasy 7.7.7.9 and classified as problematic. Affected by this vulnerability is the function deleteimg_action in the library lib/admin/image_admin.php. The manipulation of the argument imgname leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-9870	An external service interaction vulnerability in GitLab EE affecting all versions from 15.11 prior to 17.6.5, 17.7 prior to 17.7.4, and 17.8 prior to 17.8.2 allows an attacker to send requests from the GitLab server to unintended services.	4.3	More Details
CVE-2025-0516	Improper Authorization in GitLab CE/EE affecting all versions from 17.7 prior to 17.7.4, 17.8 prior to 17.8.2 allow users with limited permissions to perform unauthorized actions on critical project data.	4.3	More Details
CVE-2025-1359	A vulnerability, which was classified as problematic, has been found in SIAM Industria de Automação e Monitoramento SIAM 2.0. This issue affects some unknown processing of the file /qrcode.jsp. The manipulation of the argument url leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1358	A vulnerability classified as problematic was found in Pix Software Vivaz 6.0.10. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-1357	A vulnerability classified as problematic has been found in Seventh D-Guard up to 20250206. This affects an unknown part of the component HTTP GET Request Handler. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-26603	Vim is a greatly improved version of the good old UNIX editor Vi. Vim allows to redirect screen messages using the `:redir` ex command to register, variables and files. It also allows to show the contents of registers using the `:registers` or `:display` ex command. When redirecting the output of `:display` to a register, Vim will free the register content before storing the new content in the register. Now when redirecting the `:display` command to a register that is being displayed, Vim will free the content while shortly afterwards trying to access it, which leads to a use-after-free. Vim pre 9.1.1115 checks in the ex_display() function, that it does not try to redirect to a register while displaying this register at the same time. However this check is not complete, and so Vim does not check the `+` and `*` registers (which typically donate the X11/clipboard registers, and when a clipboard connection is not possible will fall back to use register 0 instead. In Patch 9.1.1115 Vim will therefore skip outputting to register zero when trying to redirect to the clipboard registers `*` or `+`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.2	More Details
CVE-2025-1198	An issue discovered in GitLab CE/EE affecting all versions from 16.11 prior to 17.6.5, 17.7 prior to 17.7.4, and 17.8 prior to 17.8.2 meant that long-lived connections in ActionCable potentially allowed revoked Personal Access Tokens access to streaming results.	4.2	More Details
CVE-2024-12629	In Progress® Telerik® KendoReact versions v3.5.0 through v9.4.0, an attacker can introduce or modify properties within the global prototype chain which can result in denial of service or command injection.	4.1	More Details
CVE-2024-11628	In Progress® Telerik® Kendo UI for Vue versions v2.4.0 through v6.0.1, an attacker can introduce or modify properties within the global prototype chain which can result in denial of service or command injection.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-57970	libarchive through 3.7.7 has a heap-based buffer over-read in header_gnu_longlink in archive_read_support_format_tar.c via a TAR archive because it mishandles truncation in the middle of a GNU long linkname.	4.0	More Details
CVE-2025-25201	Nitrokey 3 Firmware is the the firmware of Nitrokey 3 USB keys. For release 1.8.0, and test releases with PIV enabled prior to 1.8.0, the PIV application could accept invalid keys for authentication of the admin key. This could lead to compromise of the integrity of the data stored in the application. An attacker without access to the proper administration key would be able to generate new keys and overwrite certificates. Such an attacker would not be able to read-out or extract existing private data, nor would they be able to gain access to cryptographic operations that would normally require PIN-based authentication. The issue is fixed in piv-authenticator 0.3.9, and in Nitrokey's firmware 1.8.1.	4.0	More Details
CVE-2024-23563	HCL Connections Docs is vulnerable to a sensitive information disclosure which could allow a user to obtain sensitive information they are not entitled to, caused by improper handling of request data.	3.9	More Details
CVE-2024-31144	For a brief summary of Xapi terminology, see: https://xapi-project.github.io/xen-api/overview.html#object-model-overview Xapi contains functionality to backup and restore metadata about Virtual Machines and Storage Repositories (SRs). The metadata itself is stored in a Virtual Disk Image (VDI) inside an SR. This is used for two purposes; a general backup of metadata (e.g. to recover from a host failure if the filer is still good), and Portable SRs (e.g. using an external hard drive to move VMs to another host). Metadata is only restored as an explicit administrator action, but occurs in cases where the host has no information about the SR, and must locate the metadata VDI in order to retrieve the metadata. The metadata VDI is located by searching (in UUID alphanumeric order) each VDI, mounting it, and seeing if there is a suitable metadata file present. The first matching VDI is deemed to be the metadata VDI, and is restored from. In the general case, the content of VDIs are controlled by the VM owner, and should not be trusted by the host administrator. A malicious guest can manipulate its disk to appear to be a metadata backup. A guest cannot choose the UUIDs of its VDIs, but a guest with one disk has a 50% chance of sorting ahead of the legitimate metadata backup. A guest with two disks has a 75% chance, etc.	3.8	More Details
CVE-2024-4028	A vulnerability was found in Keycloak. This issue may allow a privileged attacker to use a malicious payload as the permission while creating items (Resource and Permissions) from the admin console, leading to a stored cross-site scripting (XSS) attack.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37020	Sequence of processor instructions leads to unexpected behavior in the Intel(R) DSA V1.0 for some Intel(R) Xeon(R) Processors may allow an authenticated user to potentially enable denial of service via local access.	3.8	More Details
CVE-2025-1341	A vulnerability, which was classified as problematic, was found in PMWeb 7.2.0. This affects an unknown part of the component Setting Handler. The manipulation leads to weak password requirements. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-1360	A vulnerability, which was classified as problematic, was found in Internet Web Solutions Sublime CRM up to 20250207. Affected is an unknown function of the file /crm/inicio.php of the component HTTP POST Request Handler. The manipulation of the argument msg_to leads to cross site scripting. It is possible to launch the attack remotely. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-1190	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as problematic. This vulnerability affects unknown code of the file /_parse/load_user-profile.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. Multiple parameters might be affected.	3.5	More Details
CVE-2025-1209	A vulnerability classified as problematic has been found in code-projects Wazifa System 1.0. Affected is the function searchuser of the file /search_resualts.php. The manipulation of the argument firstname/lastname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. There is a typo in the affected file name.	3.5	More Details
CVE-2025-1208	A vulnerability was found in code-projects Wazifa System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /Profile.php. The manipulation of the argument postcontent leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-1337	A vulnerability was found in Eastnets PaymentSafe 2.5.26.0. It has been classified as problematic. This affects an unknown part of the component BIC Search. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1195	A vulnerability, which was classified as problematic, has been found in code-projects Real Estate Property Management System 1.0. This issue affects some unknown processing of the file /Admin/EditCategory. The manipulation of the argument CategoryId leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-1196	A vulnerability, which was classified as problematic, was found in code-projects Real Estate Property Management System 1.0. Affected is an unknown function of the file /search.php. The manipulation of the argument PropertyName leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2025-1392	A vulnerability has been found in D-Link DIR-816 1.01TO and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/webproc?getpage=html/index.html&var:menu=24gwlan&var:page=24G_basic. The manipulation of the argument SSID leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2025-25899	A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11 via the 'gw' parameter at /userRpm/WanDynamicIpV6CfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	3.5	More Details
CVE-2025-1213	A vulnerability was found in pihome-shc PiHome 1.77. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument \$_SERVER['PHP_SELF'] leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-1371	A vulnerability has been found in GNU elfutils 0.192 and classified as problematic. This vulnerability affects the function handle_dynamic_symtab of the file readelf.c of the component eu-read. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The patch is identified as b38e562a4c907e08171c76b8b2def8464d5a104a. It is recommended to apply a patch to fix this issue.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1377	A vulnerability, which was classified as problematic, has been found in GNU elfutils 0.192. This issue affects the function gelf_getsymshndx of the file strip.c of the component eu-strip. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of the patch is fbf1df9ca286de3323ae541973b08449f8d03aba. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2024-39286	Incorrect execution-assigned permissions in the Linux kernel mode driver for the Intel(R) 800 Series Ethernet Driver before version 1.15.4 may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2025-1378	A vulnerability, which was classified as problematic, was found in radare2 5.9.9 33286. Affected is an unknown function in the library /libr/main/rasm2.c of the component rasm2. The manipulation leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 6.0.0 is able to address this issue. The patch is identified as c6c772d2eab692ce7ada5a4227afd50c355ad545. It is recommended to upgrade the affected component.	3.3	More Details
CVE-2025-1373	A vulnerability was found in FFmpeg up to 7.1. It has been rated as problematic. Affected by this issue is the function mov_read_trak of the file libavformat/mov.c of the component MOV Parser. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The patch is identified as 43be8d07281caca2e88bfd8ee2333633e1fb1a13. It is recommended to apply a patch to fix this issue.	3.3	More Details
CVE-2025-0503	Mattermost versions 9.11.x <= 9.11.6 fail to filter out DMs from the deleted channels endpoint which allows an attacker to infer user IDs and other metadata from deleted DMs if someone had manually marked DMs as deleted in the database.	3.1	More Details
CVE-2025-1207	A vulnerability was found in phjounin TFTP64 4.64. It has been declared as problematic. This vulnerability affects unknown code of the component DNS Handler. The manipulation leads to denial of service. The attack needs to be done within the local network. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used.	3.1	More Details
CVE-2025-27113	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a NULL pointer dereference in xmlPatMatch in pattern.c.	2.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1215	A vulnerability classified as problematic was found in vim up to 9.1.1096. This vulnerability affects unknown code of the file src/main.c. The manipulation of the argument --log leads to memory corruption. It is possible to launch the attack on the local host. Upgrading to version 9.1.1097 is able to address this issue. The patch is identified as c5654b84480822817bb7b69ebc97c174c91185e9. It is recommended to upgrade the affected component.	2.8	More Details
CVE-2024-47266	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in share file list functionality in Synology Active Backup for Business before 2.7.1-13234, 2.7.1-23234 and 2.7.1-3234 allows remote authenticated users with administrator privileges to read specific files containing non-sensitive information via unspecified vectors.	2.7	More Details
CVE-2024-39271	Improper restriction of communication channel to intended endpoints in some Intel(R) PROSet/Wireless WiFi and Killerâ„¢ WiFi software before version 23.80 may allow an unauthenticated user to potentially enable information disclosure via adjacent access.	2.6	More Details
CVE-2025-1376	A vulnerability classified as problematic was found in GNU elfutils 0.192. This vulnerability affects the function elf_strptr in the library /libelf/elf_strptr.c of the component eu-strip. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The name of the patch is b16f441cca0a4841050e3215a9f120a6d8aea918. It is recommended to apply a patch to fix this issue.	2.5	More Details
CVE-2025-1332	A vulnerability has been found in FastCMS up to 0.1.5 and classified as problematic. This vulnerability affects unknown code of the file /fastcms.html#/template/menu of the component Template Menu. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	2.4	More Details
CVE-2025-1354	A vulnerability was found in Asus RT-N12E 2.0.0.19. It has been classified as problematic. Affected is an unknown function of the file sysinfo.asp. The manipulation of the argument SSID leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-26021	Improper initialization in the firmware for some Intel(R) AMT and Intel(R) Standard Manageability may allow a privileged user to potentially enable information disclosure via local access.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25571	Improper input validation in some Intel(R) SPS firmware before SPS_E5_06.01.04.059.0 may allow a privileged user to potentially enable denial of service via local access.	2.3	More Details
CVE-2025-1368	A vulnerability was found in MicroWord eScan Antivirus 7.0.32 on Linux. It has been declared as problematic. This vulnerability affects the function ReadConfiguration of the file /opt/MicroWorld/etc/mwav.conf. The manipulation of the argument BasePath leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.3	More Details
CVE-2024-57257	A stack consumption issue in sqfs_size in Das U-Boot before 2025.01-rc1 occurs via a crafted squashfs filesystem with deep symlink nesting.	2.0	More Details
CVE-2024-46922	An issue was discovered in Samsung Mobile Processor Exynos 1480 and 2400. The absence of a null check leads to a Denial of Service at amdgpu_cs_parser_bos in the Xclipse Driver.	N/A	More Details
CVE-2025-0113	A problem with the network isolation mechanism of the Palo Alto Networks Cortex XDR Broker VM allows attackers unauthorized access to Docker containers from the host network used by Broker VM. This may allow access to read files sent for analysis and logs transmitted by the Cortex XDR Agent to the Cortex XDR server.	N/A	More Details
CVE-2025-0111	An authenticated file read vulnerability in the Palo Alto Networks PAN-OS software enables an authenticated attacker with network access to the management web interface to read files on the PAN-OS filesystem that are readable by the "nobody" user. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue does not affect Cloud NGFW or Prisma Access software.	N/A	More Details
CVE-2024-13837	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 Number	Description	Base Score	Reference
CVE-2025-25284	The ZOO-Project is an open source processing platform, released under MIT/X11 Licence. A vulnerability in ZOO-Project's WPS (Web Processing Service) implementation allows unauthorized access to files outside the intended directory through path traversal. Specifically, the Gdal_Translate service, when processing VRT (Virtual Format) files, does not properly validate file paths referenced in the VRTRasterBand element, allowing attackers to read arbitrary files on the system. The vulnerability exists because the service doesn't properly sanitize the SourceFilename parameter in VRT files, allowing relative path traversal sequences (../). When combined with VRT's raw data handling capabilities, this allows reading arbitrary files as raw binary data and converting them to TIFF format, effectively exposing their contents. This vulnerability is particularly severe because it allows attackers to read sensitive system files, potentially exposing configuration data, credentials, or other confidential information stored on the server. An unauthenticated attacker can read arbitrary files from the system through path traversal, potentially accessing sensitive information such as configuration files, credentials, or other confidential data stored on the server. The vulnerability requires no authentication and can be exploited remotely through the WPS service. This issue has been addressed in commit `5f155a8` and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-0110	A command injection vulnerability in the Palo Alto Networks PAN-OS OpenConfig plugin enables an authenticated administrator with the ability to make gNMI requests to the PAN-OS management web interface to bypass system restrictions and run arbitrary commands. The commands are run as the “__openconfig” user (which has the Device Administrator role) on the firewall. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 .	N/A	More Details
CVE-2025-0109	An unauthenticated file deletion vulnerability in the Palo Alto Networks PAN-OS management web interface enables an unauthenticated attacker with network access to the management web interface to delete certain files as the “nobody” user; this includes limited logs and configuration files but does not include system files. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue does not affect Cloud NGFW or Prisma Access software.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0108	An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-and-tricks-how-to-secure-the-management-access-of-your-palo-ba-p/464431 . This issue does not affect Cloud NGFW or Prisma Access software.	N/A	More Details
CVE-2025-25343	Tenda AC6 V15.03.05.16 firmware has a buffer overflow vulnerability in the formexeCommand function.	N/A	More Details
CVE-2025-25741	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the IPv6_PppoePassword parameter in the SetIPv6PppoeSettings module.	N/A	More Details
CVE-2025-25200	Koa is expressive middleware for Node.js using ES2017 async functions. Prior to versions 0.21.2, 1.7.1, 2.15.4, and 3.0.0-alpha.3, Koa uses an evil regex to parse the `X-Forwarded-Proto` and `X-Forwarded-Host` HTTP headers. This can be exploited to carry out a Denial-of-Service attack. Versions 0.21.2, 1.7.1, 2.15.4, and 3.0.0-alpha.3 fix the issue.	N/A	More Details
CVE-2025-25746	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the Password parameter in the SetWanSettings module.	N/A	More Details
CVE-2025-26623	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. A heap buffer overflow was found in Exiv2 versions v0.28.0 to v0.28.4. Versions prior to v0.28.0, such as v0.27.7, are **not** affected. Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The heap overflow is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `fixiso`. The bug is fixed in version v0.28.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25744	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the Password parameter in the SetDynamicDNSSettings module.	N/A	More Details
CVE-2024-46923	An issue was discovered in Samsung Mobile Processor Exynos 2200, 1480, and 2400. The absence of a null check leads to a Denial of Service at amdgpu_cs_ib_fill in the Xclipse Driver.	N/A	More Details
CVE-2024-57055	Server-Side Access Control Bypass vulnerability in WombatDialer before 25.02 could allow unauthorized users to potentially call certain services without the necessary access level. This issue is limited to services used by the client (not the general-use JSON services) and requires reverse engineering of the proprietary serialization protocol, making it difficult to exploit.	N/A	More Details
CVE-2025-21608	Meshtastic is an open source mesh networking solution. In affected firmware versions crafted packets over MQTT are able to appear as a DM in client to a node even though they were not decoded with PKC. This issue has been addressed in version 2.5.19 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-51122	Cross Site Scripting vulnerability in Zertificon Z1 SecureMail Z1 CertServer v.3.16.4-2516-debian12 allows a remote attacker to execute arbitrary code via the ST, L, O, OU, CN parameters.	N/A	More Details
CVE-2024-55460	A time-based SQL injection vulnerability in the login page of BoardRoom Limited Dividend Distribution Tax Election System Version v2.0 allows attackers to execute arbitrary code via a crafted input.	N/A	More Details
CVE-2022-41545	The administrative web interface of a Netgear C7800 Router running firmware version 6.01.07 (and possibly others) authenticates users via basic authentication, with an HTTP header containing a base64 value of the plaintext username and password. Because the web server also does not utilize transport security by default, this renders the administrative credentials vulnerable to eavesdropping by an adversary during every authenticated request made by a client to the router over a WLAN, or a LAN, should the adversary be able to perform a man-in-the-middle attack.	N/A	More Details
CVE-2024-57602	An issue in Alex Tselegidis EasyAppointments v.1.5.0 allows a remote attacker to escalate privileges via the index.php file.	N/A	More Details
CVE-2024-57601	Cross Site Scripting vulnerability in Alex Tselegidis EasyAppointments v.1.5.0 allows a remote attacker to execute arbitrary code via the legal_settings parameter.	N/A	More Details
CVE-2024-56940	An issue in the profile image upload function of LearnDash v6.7.1 allows attackers to cause a Denial of Service (DoS) via excessive file uploads.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50608	An issue was discovered in Fluent Bit 3.1.9. When the Prometheus Remote Write input plugin is running and listening on an IP address and port, one can send a packet with Content-Length: 0 and it crashes the server. Improper handling of the case when Content-Length is 0 allows a user (with access to the endpoint) to perform a remote Denial of service attack. The crash happens because of a NULL pointer dereference when 0 (from the Content-Length) is passed to the function <code>cfl_sds_len</code> , which in turn tries to cast a NULL pointer into struct <code>cfl_sds</code> . This is related to <code>process_payload_metrics_ng()</code> at <code>prom_rw_prot.c</code> .	N/A	More Details
CVE-2024-50609	An issue was discovered in Fluent Bit 3.1.9. When the OpenTelemetry input plugin is running and listening on an IP address and port, one can send a packet with Content-Length: 0 and it crashes the server. Improper handling of the case when Content-Length is 0 allows a user (with access to the endpoint) to perform a remote Denial of service attack. The crash happens because of a NULL pointer dereference when 0 (from the Content-Length) is passed to the function <code>cfl_sds_len</code> , which in turn tries to cast a NULL pointer into struct <code>cfl_sds</code> . This is related to <code>process_payload_traces_proto_ng()</code> at <code>opentelemetry_prot.c</code> .	N/A	More Details
CVE-2024-51440	An issue in Nothing Tech Nothing OS v.2.6 allows a local attacker to escalate privileges via the <code>NtBpfService</code> component.	N/A	More Details
CVE-2024-56882	Sage DPW before 2024_12_000 is vulnerable to Cross Site Scripting (XSS). Low-privileged Sage users with employee role privileges can permanently store JavaScript code in the <code>Kurstitel</code> and <code>Kurzinfo</code> input fields. The injected payload is executed for each authenticated user who views and interacts with the modified data elements.	N/A	More Details
CVE-2024-56883	Sage DPW before 2024_12_001 is vulnerable to Incorrect Access Control. The implemented role-based access controls are not always enforced on the server side. Low-privileged Sage users with employee role privileges can create external courses for other employees, even though they do not have the option to do so in the user interface. To do this, a valid request to create a course simply needs to be modified, so that the current user ID in the "id" parameter is replaced with the ID of another user.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25300	smartbanner.js is a customizable smart app banner for iOS and Android. Prior to version 1.14.1, clicking on smartbanner `View` link and navigating to 3rd party page leaves `window.opener` exposed. It may allow hostile third parties to abuse `window.opener`, e.g. by redirection or injection on the original page with smartbanner. `rel="noopener"` is automatically populated to links as of `v1.14.1` which is a recommended upgrade to resolve the vulnerability. Some workarounds are available for those who cannot upgrade. Ensure `View` link is only taking users to App Store or Google Play Store where security is guarded by respective app store security teams. If `View` link is going to a third party page, limit smartbanner.js to be used on iOS that decreases the scope of the vulnerability since as of Safari 12.1, `rel="noopener"` is imposed on all `target="_blank"` links. Version 1.14.1 of smartbanner.js contains a fix for the issue.	N/A	More Details
CVE-2025-26058	Webkul QloApps v1.6.1 exposes authentication tokens in URLs during redirection. When users access the admin panel or other protected areas, the application appends sensitive authentication tokens directly to the URL.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26620	Duende.AccessTokenManagement is a set of .NET libraries that manage OAuth and OpenId Connect access tokens. Duende.AccessTokenManagement contains a race condition when requesting access tokens using the client credentials flow. Concurrent requests to obtain an access token using differing protocol parameters can return access tokens obtained with the wrong scope, resource indicator, or other protocol parameters. Such usage is somewhat atypical, and only a small percentage of users are likely to be affected. Duende.AccessTokenManagement can request access tokens using the client credentials flow in several ways. In basic usage, the client credentials flow is configured once and the parameters do not vary. In more advanced situations, requests with varying protocol parameters may be made by calling specific overloads of these methods: <code>`HttpContext.GetClientAccessTokenAsync()`</code> and <code>`IClientCredentialsTokenManagementService.GetAccessTokenAsync()`</code>. There are overloads of both of these methods that accept a <code>`TokenRequestParameters`</code> object that customizes token request parameters. However, concurrent requests with varying <code>`TokenRequestParameters`</code> will result in the same token for all concurrent calls. Most users can simply update the NuGet package to the latest version. Customizations of the <code>`IClientCredentialsTokenCache`</code> that derive from the default implementation (<code>`DistributedClientCredentialsTokenCache`</code>) will require a small code change, as its constructor was changed to add a dependency on the <code>`ITokenRequestSynchronization`</code> service. The synchronization service will need to be injected into the derived class and passed to the base constructor. The impact of this vulnerability depends on how Duende.AccessTokenManagement is used and on the security architecture of the solution. Most users will not be vulnerable to this issue. More advanced users may run into this issue by calling the methods specified above with customized token request parameters. The impact of obtaining an access token with different than intended protocol parameters will vary depending on application logic, security architecture, and the authorization policy of the resource servers.	N/A	More Details
CVE-2024-51123	An issue in Zertificon Z1 SecureMail Z1 SecureMail Gateway 4.44.2-7240-debian12 allows a remote attacker to obtain sensitive information via the <code>/compose-pdf.xhtml?convid=[id]</code> component.	N/A	More Details
CVE-2025-26605	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, <code>`deletar_cargo.php`</code> endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25743	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a command injection vulnerability in the SetVirtualServerSettings module.	N/A	More Details
CVE-2025-26608	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `dependente_docdependente.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26606	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `informacao_adicional.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-22919	A reachable assertion in FFmpeg git-master commit N-113007-g8d24a28d06 allows attackers to cause a Denial of Service (DoS) via opening a crafted AAC file.	N/A	More Details
CVE-2025-25896	A buffer overflow vulnerability was discovered in D-Link DSL-3782 v1.01 via the destination, netmask, and gateway parameters. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	N/A	More Details
CVE-2025-25184	Rack provides an interface for developing web applications in Ruby. Prior to versions 2.2.11, 3.0.12, and 3.1.10, Rack::CommonLogger can be exploited by crafting input that includes newline characters to manipulate log entries. The supplied proof-of-concept demonstrates injecting malicious content into logs. When a user provides the authorization credentials via Rack::Auth::Basic, if success, the username will be put in env['REMOTE_USER'] and later be used by Rack::CommonLogger for logging purposes. The issue occurs when a server intentionally or unintentionally allows a user creation with the username contain CRLF and white space characters, or the server just want to log every login attempts. If an attacker enters a username with CRLF character, the logger will log the malicious username with CRLF characters into the logfile. Attackers can break log formats or insert fraudulent entries, potentially obscuring real activity or injecting malicious data into log files. Versions 2.2.11, 3.0.12, and 3.1.10 contain a fix.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0925	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-0818. Reason: This candidate is a reservation duplicate of CVE-2025-0818. Notes: All CVE users should reference CVE-2025-0818 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-0919	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-0818. Reason: This candidate is a reservation duplicate of CVE-2025-0818. Notes: All CVE users should reference CVE-2025-0818 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-21698	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-32838	SQL Injection vulnerability in various API endpoints - offices, dashboards, etc. Apache Fineract versions 1.9 and before have a vulnerability that allows an authenticated attacker to inject malicious data into some of the REST API endpoints' query parameter. Users are recommended to upgrade to version 1.10.1, which fixes this issue. A SQL Validator has been implemented which allows us to configure a series of tests and checks against our SQL queries that will allow us to validate and protect against nearly all potential SQL injection attacks.	N/A	More Details
CVE-2023-49780	Cross-site scripting vulnerability exists in acmailer CGI ver.4.0.5 and earlier. An arbitrary script may be executed on the web browser of the user who accessed the management page of the affected product.	N/A	More Details
CVE-2025-22920	A heap buffer overflow vulnerability in FFmpeg before commit 4bf784c allows attackers to trigger a memory corruption via supplying a crafted media file in avformat when processing tile grid group streams. This can lead to a Denial of Service (DoS).	N/A	More Details
CVE-2025-26607	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `documento_excluir.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1243	The Temporal api-go library prior to version 1.44.1 did not send `update response` information to Data Converter when the proxy package within the api-go module was used in a gRPC proxy prior to transmission. This resulted in information contained within the `update response` field not having Data Converter transformations (e.g. encryption) applied. This is an issue only when using the UpdateWorkflowExecution APIs (released on 13th January 2025) with a proxy leveraging the api-go library before version 1.44.1. Other data fields were correctly sent to Data Converter. This issue does not impact the Data Converter server. Data was encrypted in transit. Temporal Cloud services are not impacted.	N/A	More Details
CVE-2025-25471	FFmpeg git master before commit fd1772 was discovered to contain a NULL pointer dereference via the component libavformat/mov.c.	N/A	More Details
CVE-2025-25472	A buffer overflow in DCMTK git master v3.6.9+ DEV allows attackers to cause a Denial of Service (DoS) via a crafted DCM file.	N/A	More Details
CVE-2025-25473	FFmpeg git master before commit c08d30 was discovered to contain a NULL pointer dereference via the component libavformat/mov.c.	N/A	More Details
CVE-2025-25474	DCMTK v3.6.9+ DEV was discovered to contain a buffer overflow via the component /dcmimgle/diinpvt.h.	N/A	More Details
CVE-2025-25475	A NULL pointer dereference in the component /libsrc/dcrleccd.cc of DCMTK v3.6.9+ DEV allows attackers to cause a Denial of Service (DoS) via a crafted DICOM file.	N/A	More Details
CVE-2025-26624	Rufus is a utility that helps format and create bootable USB flash drives. A DLL hijacking vulnerability in Rufus 4.6.2208 and earlier versions allows an attacker loading and executing a malicious DLL with escalated privileges (since the executable has been granted higher privileges during the time of launch) due to the ability to inject a malicious `cfgmgr32.dll` in the same directory as the executable and have it side load automatically. This is fixed in commit `74dfa49`, which will be part of version 4.7. Users are advised to upgrade as soon as version 4.7 becomes available. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-25895	An OS command injection vulnerability was discovered in D-Link DSL-3782 v1.01 via the public_type parameter. This vulnerability allows attackers to execute arbitrary operating system (OS) commands via a crafted packet.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25894	An OS command injection vulnerability was discovered in D-Link DSL-3782 v1.01 via the samba_wg and samba_nbn parameters. This vulnerability allows attackers to execute arbitrary operating system (OS) commands via a crafted packet.	N/A	More Details
CVE-2025-25893	An OS command injection vulnerability was discovered in D-Link DSL-3782 v1.01 via the inIP, insPort, inePort, exsPort, exePort, and protocol parameters. This vulnerability allows attackers to execute arbitrary operating system (OS) commands via a crafted packet.	N/A	More Details
CVE-2025-25892	A buffer overflow vulnerability was discovered in D-Link DSL-3782 v1.01 via the sstartip, sendip, dstartip, and dendip parameters. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	N/A	More Details
CVE-2024-57604	An issue in MaysWind ezBookkeeping 0.7.0 allows a remote attacker to escalate privileges via the token component.	N/A	More Details
CVE-2025-26609	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `familiar_docfamiliar.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26610	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `restaurar_produto_desocultar.php` endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26611	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `remover_produto.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26612	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `adicionar_almoxarife.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26613	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. An OS Command Injection vulnerability was discovered in the WeGIA application, `gerenciar_backup.php` endpoint. This vulnerability could allow an attacker to execute arbitrary code remotely. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26614	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `deletar_documento.php` endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26616	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Path Traversal vulnerability was discovered in the WeGIA application, `exportar_dump.php` endpoint. This vulnerability could allow an attacker to gain unauthorized access to sensitive information stored in `config.php`. `config.php` contains information that could allow direct access to the database. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-26617	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `historico_paciente.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2025-25742	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the AccountPassword parameter in the SetSysEmailSettings module.	N/A	More Details
CVE-2025-22921	FFmpeg git-master,N-113007-g8d24a28d06 was discovered to contain a segmentation violation via the component /libavcodec/jpeg2000dec.c.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25467	Insufficient tracking and releasing of allocated used memory in libx264 git master allows attackers to execute arbitrary code via creating a crafted AAC file.	N/A	More Details
CVE-2025-25468	FFmpeg git-master before commit d5873b was discovered to contain a memory leak in the component libavutil/mem.c.	N/A	More Details
CVE-2025-25469	FFmpeg git-master before commit d5873b was discovered to contain a memory leak in the component libavutil/iamf.c.	N/A	More Details
CVE-2025-25891	A buffer overflow vulnerability was discovered in D-Link DSL-3782 v1.01, triggered by the destination, netmask and gateway parameters. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	N/A	More Details
CVE-2025-22207	Improperly built order clauses lead to a SQL injection vulnerability in the backend task list of com_scheduler.	N/A	More Details
CVE-2024-57049	A vulnerability in the TP-Link Archer c20 router with firmware version V6.6_230412 and earlier permits unauthorized individuals to bypass the authentication of some interfaces under the /cgi directory. When adding Referer: http://tplinkwifi.net to the the request, it will be recognized as passing the authentication.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-21702	In the Linux kernel, the following vulnerability has been resolved: pfifo_tail_enqueue: Drop new packet when sch->limit == 0 Expected behaviour: In case we reach scheduler's limit, pfifo_tail_enqueue() will drop a packet in scheduler's queue and decrease scheduler's qlen by one. Then, pfifo_tail_enqueue() enqueue new packet and increase scheduler's qlen by one. Finally, pfifo_tail_enqueue() return `NET_XMIT_CN` status code. Weird behaviour: In case we set `sch->limit == 0` and trigger pfifo_tail_enqueue() on a scheduler that has no packet, the 'drop a packet' step will do nothing. This means the scheduler's qlen still has value equal 0. Then, we continue to enqueue new packet and increase scheduler's qlen by one. In summary, we can leverage pfifo_tail_enqueue() to increase qlen by one and return `NET_XMIT_CN` status code. The problem is: Let's say we have two qdiscs: Qdisc_A and Qdisc_B. - Qdisc_A's type must have '->graft()' function to create parent/child relationship. Let's say Qdisc_A's type is `hfsc`. Enqueue packet to this qdisc will trigger `hfsc_enqueue`. - Qdisc_B's type is pfifo_head_drop. Enqueue packet to this qdisc will trigger `pfifo_tail_enqueue`. - Qdisc_B is configured to have `sch->limit == 0`. - Qdisc_A is configured to route the enqueued's packet to Qdisc_B. Enqueue packet through Qdisc_A will lead to: - hfsc_enqueue(Qdisc_A) -> pfifo_tail_enqueue(Qdisc_B) - Qdisc_B->q.qlen += 1 - pfifo_tail_enqueue() return `NET_XMIT_CN` - hfsc_enqueue() check for `NET_XMIT_SUCCESS` and see `NET_XMIT_CN` => hfsc_enqueue() don't increase qlen of Qdisc_A. The whole process lead to a situation where Qdisc_A->q.qlen == 0 and Qdisc_B->q.qlen == 1. Replace 'hfsc' with other type (for example: 'drr') still lead to the same problem. This violate the design where parent's qlen should equal to the sum of its childrens'qlen. Bug impact: This issue can be used for user->kernel privilege escalation when it is reachable.	N/A	More Details
CVE-2024-56973	Insecure Permissions vulnerability in Alvaria, Inc Unified IP Unified Director before v.7.2SP2 allows a remote attacker to execute arbitrary code via the source and filename parameters to the ProcessUploadFromURL.jsp component.	N/A	More Details
CVE-2025-25304	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. Prior to version 5.26.0 of vega and 5.4.2 of vega-selections, the `vSelectionTuples` function can be used to call JavaScript functions, leading to cross-site scripting. `vSelectionTuples` calls multiple functions that can be controlled by an attacker, including one call with an attacker-controlled argument. This can be used to call `Function()` with arbitrary JavaScript and the resulting function can be called with `vSelectionTuples` or using a type coercion to call `toString` or `valueOf`. Version 5.26.0 of vega and 5.4.2 of vega-selections fix this issue.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26508	Certain HP LaserJet Pro, HP LaserJet Enterprise, and HP LaserJet Managed Printers may potentially be vulnerable to Remote Code Execution and Elevation of Privilege when processing a PostScript print job.	N/A	More Details
CVE-2025-26507	Certain HP LaserJet Pro, HP LaserJet Enterprise, and HP LaserJet Managed Printers may potentially be vulnerable to Remote Code Execution and Elevation of Privilege when processing a PostScript print job.	N/A	More Details
CVE-2025-26506	Certain HP LaserJet Pro, HP LaserJet Enterprise, and HP LaserJet Managed Printers may potentially be vulnerable to Remote Code Execution and Elevation of Privilege when processing a PostScript print job.	N/A	More Details
CVE-2025-25295	Label Studio is an open source data labeling tool. A path traversal vulnerability in Label Studio SDK versions prior to 1.0.10 allows unauthorized file access outside the intended directory structure. The flaw exists in the VOC, COCO and YOLO export functionalities. These functions invoke a `download` function on the `label-studio-sdk` python package, which fails to validate file paths when processing image references during task exports. By creating tasks with path traversal sequences in the image field, an attacker can force the application to read files from arbitrary server filesystem locations when exporting projects in any of the mentioned formats. This is authentication-required vulnerability allowing arbitrary file reads from the server filesystem. It may lead to potential exposure of sensitive information like configuration files, credentials, and confidential data. Label Studio versions before 1.16.0 specified SDK versions prior to 1.0.10 as dependencies, and the issue was confirmed in Label Studio version 1.13.2.dev0; therefore, Label Studio users should upgrade to 1.16.0 or newer to mitigate it.	N/A	More Details
CVE-2024-57790	IXON B.V. IXrouter IX2400 (Industrial Edge Gateway) v3.0 was discovered to contain hardcoded root credentials stored in the non-volatile flash memory. This vulnerability allows physically proximate attackers to gain root access via UART or SSH.	N/A	More Details
CVE-2024-3220	There is a defect in the CPython standard library module “mimetypes” where on Windows the default list of known file locations are writable meaning other users can create invalid files to cause MemoryError to be raised on Python runtime startup or have file extensions be interpreted as the incorrect file type. This defect is caused by the default locations of Linux and macOS platforms (such as “/etc/mime.types”) also being used on Windows, where they are user-writable locations (“C:\etc\mime.types”). To work-around this issue a user can call mimetypes.init() with an empty list (“[]”) on Windows platforms to avoid using the default list of known file locations.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25740	D-Link DIR-853 A1 FW1.20B07 was discovered to contain a stack-based buffer overflow vulnerability via the PSK parameter in the SetQuickVPNSettings module.	N/A	More Details
CVE-2024-4282	Brocade SANnav OVA before SANnav 2.3.1b enables SHA1 deprecated setting for SSH for port 22.	N/A	More Details
CVE-2025-1239	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS allows Stored XSS via the Blocked Sites list. This vulnerability requires an authenticated administrator session to a locally managed Firebox.This issue affects Fireware OS: from 12.0 through 12.5.12+701324, from 12.6 through 12.11.	N/A	More Details
CVE-2025-1071	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS allows Stored XSS via the spamBlocker module. This vulnerability requires an authenticated administrator session to a locally managed Firebox.This issue affects Fireware OS: from 12.0 through 12.5.12+701324, from 12.6 through 12.11.	N/A	More Details
CVE-2025-0178	Improper Input Validation vulnerability in WatchGuard Fireware OS allows an attacker to manipulate the value of the HTTP Host header in requests sent to the Web UI. An attacker could exploit this vulnerability to redirect users to malicious websites, poison the web cache, or inject malicious JavaScript into responses sent by the Web UI. This issue affects Fireware OS: from 12.0 up to and including 12.11.	N/A	More Details
CVE-2025-26524	This vulnerability exists in RupeeWeb trading platform due to missing rate limiting on OTP requests in certain API endpoints. An authenticated remote attacker could exploit this vulnerability by sending multiple OTP request through vulnerable API endpoints which could lead to the OTP bombing/ flooding on the targeted system.	N/A	More Details
CVE-2025-26523	This vulnerability exists in RupeeWeb trading platform due to insufficient authorization controls on certain API endpoints handling addition and deletion operations. Successful exploitation of this vulnerability could allow an authenticated remote attacker to modify information belonging to other user accounts.	N/A	More Details
CVE-2025-26522	This vulnerability exists in RupeeWeb trading platform due to improper implementation of OTP validation mechanism in certain API endpoints. A remote attacker with valid credentials could exploit this vulnerability by manipulating API responses. Successful exploitation of this vulnerability could allow the attacker to bypass Two-Factor Authentication (2FA) for other user accounts.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52577	In Apache Ignite versions from 2.6.0 and before 2.17.0, configured Class Serialization Filters are ignored for some Ignite endpoints. The vulnerability could be exploited if an attacker manually crafts an Ignite message containing a vulnerable object whose class is present in the Ignite server classpath and sends it to Ignite server endpoints. Deserialization of such a message by the Ignite server may result in the execution of arbitrary code on the Apache Ignite server side.	N/A	More Details
CVE-2024-10405	Brocade SANnav before SANnav 2.3.1b enables weak TLS ciphers on ports 443 and 18082. In case of a successful exploit, an attacker can read Brocade SANnav data stream that includes monitored Brocade Fabric OS switches performance data, port status, zoning information, WWNs, IP Addresses, but no customer data, no personal data and no secrets or passwords, as it travels across the network.	N/A	More Details
CVE-2024-5461	Implementation of the Simple Network Management Protocol (SNMP) operating on the Brocade 6547 (FC5022) embedded switch blade, makes internal script calls to system.sh from within the SNMP binary. An authenticated attacker could perform command or parameter injection on SNMP operations that are only enabled on the Brocade 6547 (FC5022) embedded switch. This injection could allow the authenticated attacker to issue commands as Root.	N/A	More Details
CVE-2024-57050	A vulnerability in the TP-Link WR840N v6 router with firmware version 0.9.1 4.16 and earlier permits unauthorized individuals to bypass the authentication of some interfaces under the /cgi directory. When adding Referer: http://tplinkwifi.net to the the request, it will be recognized as passing the authentication.	N/A	More Details
CVE-2025-25224	The LuxCal Web Calendar prior to 5.3.3M (MySQL version) and prior to 5.3.3L (SQLite version) contains a missing authentication vulnerability in dloader.php. If this vulnerability is exploited, arbitrary files on a server may be obtained.	N/A	More Details
CVE-2024-13726	The Coder WordPress plugin through 1.3.4 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	N/A	More Details
CVE-2021-46686	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in acmailer CGI ver.4.0.3 and earlier and acmailer DB ver.1.1.5 and earlier. If this vulnerability is exploited, an arbitrary OS command may be executed by an attacker.	N/A	More Details
CVE-2025-20075	Server-side request forgery (SSRF) vulnerability exists in FileMegane versions above 3.0.0.0 prior to 3.4.0.0. Executing arbitrary backend Web API requests could potentially lead to rebooting the services.	N/A	More Details
CVE-2025-25055	Authentication bypass by spoofing issue exists in FileMegane versions above 1.0.0.0 prior to 3.4.0.0, which may lead to user impersonation. If exploited, restricted file contents may be accessed.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-25221	The LuxCal Web Calendar prior to 5.3.3M (MySQL version) and prior to 5.3.3L (SQLite version) contains an SQL injection vulnerability in pdf.php. If this vulnerability is exploited, information in a database may be deleted, altered, or retrieved.	N/A	More Details
CVE-2025-25222	The LuxCal Web Calendar prior to 5.3.3M (MySQL version) and prior to 5.3.3L (SQLite version) contains an SQL injection vulnerability in retrieve.php. If this vulnerability is exploited, information in a database may be deleted, altered, or retrieved.	N/A	More Details
CVE-2025-25223	The LuxCal Web Calendar prior to 5.3.3M (MySQL version) and prior to 5.3.3L (SQLite version) contains a path traversal vulnerability in dloader.php. If this vulnerability is exploited, arbitrary files on a server may be obtained.	N/A	More Details
CVE-2024-13627	The OWL Carousel Slider WordPress plugin through 2.2 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.	N/A	More Details
CVE-2024-5462	If Brocade Fabric OS before Fabric OS 9.2.0 configuration settings are not set to encrypt SNMP passwords, then the SNMP privsecret / authsecret fields can be exposed in plaintext. The plaintext passwords can be exposed in a configupload capture or a supportsave capture if encryption of passwords is not enabled. An attacker can use these passwords to fetch values of the supported OIDs via SNMPv3 queries. There are also a limited number of MIB objects that can be modified.	N/A	More Details
CVE-2024-13626	The VR-Frases (collect & share quotes) WordPress plugin through 3.0.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	N/A	More Details
CVE-2024-13625	The Tube Video Ads Lite WordPress plugin through 1.5.7 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.	N/A	More Details
CVE-2024-13608	The Track Logins WordPress plugin through 1.0 does not sanitize and escape a parameter before using it in a SQL statement, allowing admins to perform SQL injection attacks	N/A	More Details
CVE-2025-26700	Authentication bypass using an alternate path or channel issue exists in "RoboForm Password Manager" App for Android versions prior to 9.7.4, which may allow an attacker with access to a device where the application is installed to bypass the lock screen and obtain sensitive information.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-26793	The Web GUI configuration panel of Hirsch (formerly Identiv and Viscount) Enterphone MESH through 2024 ships with default credentials (username freedom, password viscount). The administrator is not prompted to change these credentials on initial configuration, and changing the credentials requires many steps. Attackers can use the credentials over the Internet via mesh.webadmin.MESHAdminServlet to gain access to dozens of Canadian and U.S. apartment buildings and obtain building residents' PII. NOTE: the Supplier's perspective is that the "vulnerable systems are not following manufacturers' recommendations to change the default password."	N/A	More Details
CVE-2024-37375	Rejected reason: This CVE record has been withdrawn due to a duplicate entry CVE-2024-13843.	N/A	More Details
CVE-2024-37374	Rejected reason: This CVE record has been withdrawn due to a duplicate entry CVE-2024-13842.	N/A	More Details
CVE-2025-26789	An issue was discovered in Logpoint AgentX before 1.5.0. A vulnerability caused by limited access controls allowed li-admin users to access sensitive information about AgentX Manager in a Logpoint deployment.	N/A	More Details
CVE-2025-23406	Out-of-bounds read vulnerability caused by improper checking of TCP MSS option values exists in Cente middleware TCP/IP Network Series, which may lead to processing a specially crafted packet to cause the affected product crashed.	N/A	More Details
CVE-2024-2240	Docker daemon in Brocade SANnav before SANnav 2.3.1b runs without auditing. The vulnerability could allow a remote authenticated attacker to execute various attacks.	N/A	More Details
CVE-2024-13125	The Everest Forms WordPress plugin before 3.0.8.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	More Details
CVE-2025-0981	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to hijack a user's session by exploiting a Stored Cross Site Scripting (XSS) vulnerability in the Group Editor page. This allows admin users to inject malicious JavaScript, which captures the session cookie of authenticated users. The cookie can then be sent to an external server, enabling session hijacking. It can also lead to information disclosure, as exposed session cookies can be used to impersonate users and gain unauthorised access to sensitive information.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-1023	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a time-based blind SQL Injection vulnerability in the EditEventTypes functionality. The newCountName parameter is directly concatenated into an SQL query without proper sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion.	N/A	More Details
CVE-2023-34399	Mercedes-Benz head-unit NTG6 contains functions to import or export profile settings over USB. Some values of this table are serialized archive according boost library. The version of boost library contains vulnerability integer overflow.	N/A	More Details
CVE-2023-34398	Mercedes-Benz head-unit NTG6 contains functions to import or export profile settings over USB. Some values of this table are serialized archive according boost library. The boost library contains a vulnerability/null pointer dereference.	N/A	More Details
CVE-2023-34397	Mercedes Benz head-unit NTG 6 contains functions to import or export profile settings over USB. During parsing you can trigger that the service will be crashed.	N/A	More Details
CVE-2025-21701	In the Linux kernel, the following vulnerability has been resolved: net: avoid race between device unregistration and ethnl ops The following trace can be seen if a device is being unregistered while its number of channels are being modified. DEBUG_LOCKS_WARN_ON(lock->magic != lock) WARNING: CPU: 3 PID: 3754 at kernel/locking/mutex.c:564 __mutex_lock+0xc8a/0x1120 CPU: 3 UID: 0 PID: 3754 Comm: ethtool Not tainted 6.13.0-rc6+ #771 RIP: 0010:__mutex_lock+0xc8a/0x1120 Call Trace: <TASK> ethtool_check_max_channel+0x1ea/0x880 ethnl_set_channels+0x3c3/0xb10 ethnl_default_set_doit+0x306/0x650 genl_family_rcv_msg_doit+0x1e3/0x2c0 genl_rcv_msg+0x432/0x6f0 netlink_rcv_skb+0x13d/0x3b0 genl_rcv+0x28/0x40 netlink_unicast+0x42e/0x720 netlink_sendmsg+0x765/0xc20 __sys_sendto+0x3ac/0x420 __x64_sys_sendto+0xe0/0x1c0 do_syscall_64+0x95/0x180 entry_SYSCALL_64_after_hwframe+0x76/0x7e This is because unregister_netdevice_many_notify might run before the rtnl lock section of ethnl operations, eg. set_channels in the above example. In this example the rss lock would be destroyed by the device unregistration path before being used again, but in general running ethnl operations while dismantle has started is not a good idea. Fix this by denying any operation on devices being unregistered. A check was already there in ethnl_ops_begin, but not wide enough. Note that the same issue cannot be seen on the ioctl version (__dev_ethtool) because the device reference is retrieved from within the rtnl lock section there. Once dismantle started, the net device is unlisted and no reference will be found.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0692	The Simple Video Management System WordPress plugin through 1.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	More Details
CVE-2024-13121	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content WordPress plugin before 4.15.20 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	More Details
CVE-2025-1053	Under certain error conditions at time of SANnav installation or upgrade, the encryption key can be written into and obtained from a Brocade SANnav supportsave. An attacker with privileged access to the Brocade SANnav database could use the encryption key to obtain passwords used by Brocade SANnav.	N/A	More Details
CVE-2024-13120	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content WordPress plugin before 4.15.20 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	More Details
CVE-2024-12586	The Chalet-Montagne.com Tools WordPress plugin through 2.7.8 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.	N/A	More Details
CVE-2024-34521	A directory traversal vulnerability exists in the Mavenir SCE Application Provisioning Portal, version PORTAL-LBS-R_1_0_24_0, which allows an administrative user to access system files with the file permissions of the privileged system user running the application.	N/A	More Details
CVE-2024-57605	Cross Site Scripting vulnerability in Daylight Studio Fuel CMS v.1.5.2 allows an attacker to escalate privileges via the /fuel/blocks/ and /fuel/pages components.	N/A	More Details
CVE-2024-57045	A vulnerability in the D-Link DIR-859 router with firmware version A3 1.05 and earlier permits unauthorized individuals to bypass the authentication. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page.	N/A	More Details
CVE-2024-57046	A vulnerability in the Netgear DGN2200 router with firmware version v1.0.0.46 and earlier permits unauthorized individuals to bypass the authentication. When adding "?x=1.gif" to the the requested url, it will be recognized as passing the authentication.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30369	Rejected reason: Was determined not a vulnerability.	N/A	More Details
CVE-2023-34400	Mercedes-Benz head-unit NTG6 contains functions to import or export profile settings over USB. In case of parsing file, service try to define header inside the file and convert it to null-terminated string. If character is missed, will return null pointer.	N/A	More Details
CVE-2024-57378	Wazuh SIEM version 4.8.2 is affected by a broken access control vulnerability. This issue allows the unauthorized creation of internal users without assigning any existing user role, potentially leading to privilege escalation or unauthorized access to sensitive resources.	N/A	More Details
CVE-2023-34401	Mercedes-Benz head-unit NTG6 contains functions to import or export profile settings over USB. Inside profile folder there is a file, which is encoded with proprietary UD2 codec. Due to missed size checks in the enapsulate file, attacker can achieve Out-of-Bound Read in heap memory.	N/A	More Details
CVE-2023-34402	Mercedes-Benz head-unit NTG6 contains functions to import or export profile settings over USB. Inside file is encapsulate another file, which service will drop during processing. Due to missed checks, attacker can achieve Arbitrary File Write with service speech rights.	N/A	More Details
CVE-2024-45320	Out-of-bounds write vulnerability exists in DocuPrint CP225w 01.22.01 and earlier, DocuPrint CP228w 01.22.01 and earlier, DocuPrint CM225fw 01.10.01 and earlier, and DocuPrint CM228fw 01.10.01 and earlier. If an affected MFP processes a specially crafted printer job file, a denial-of-service (DoS) condition may occur.	N/A	More Details
CVE-2025-22961	A critical information disclosure vulnerability exists in the web-based management interface of GatesAir Maxiva UAXT, VAXT transmitters due to Incorrect Access Control (CWE-284). Unauthenticated attackers can directly access sensitive database backup files (snapshot_users.db) via publicly exposed URLs (/logs/devcfg/snapshot/ and /logs/devcfg/user/). Exploiting this vulnerability allows retrieval of sensitive user data, including login credentials, potentially leading to full system compromise.	N/A	More Details
CVE-2025-22960	A session hijacking vulnerability exists in the web-based management interface of GatesAir Maxiva UAXT, VAXT transmitters. Unauthenticated attackers can access exposed log files (/logs/debug/xteLog*), potentially revealing sensitive session-related information such as session IDs (sess_id) and authentication success tokens (user_check_password OK). Exploiting this flaw could allow attackers to hijack active sessions, gain unauthorized access, and escalate privileges on affected devices.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-57782	An issue in Docker-proxy v18.09.0 allows attackers to cause a denial of service.	N/A	More Details
CVE-2024-56908	In Perfex Crm < 3.2.1, an authenticated attacker can send a crafted HTTP POST request to the affected upload_sales_file endpoint. By providing malicious input in the rel_id parameter, combined with improper input validation, the attacker can bypass restrictions and upload arbitrary files to directories of their choice, potentially leading to remote code execution or server compromise.	N/A	More Details
CVE-2024-53311	A Stack buffer overflow in the arguments parameter in Immunity Inc. Immunity Debugger v1.85 allows attackers to execute arbitrary code via a crafted input that exceeds the buffer size.	N/A	More Details
CVE-2024-53310	A Structured Exception Handler based buffer overflow vulnerability exists in Effectmatrix Total Video Converter Command Line (TVCC) 2.50 when a specially crafted file is passed to the -ff parameter. The vulnerability occurs due to improper handling of file input with overly long characters, leading to memory corruption. This can result in arbitrary code execution or denial of service.	N/A	More Details
CVE-2024-53309	A stack-based buffer overflow vulnerability exists in Effectmatrix Total Video Converter Command Line (TVCC) 2.50 when an overly long string is passed to the "-f" parameter. This can lead to memory corruption, potentially allowing arbitrary code execution or causing a denial of service via specially crafted input.	N/A	More Details
CVE-2023-34406	An issue was discovered on Mercedes Benz NTG 6. A possible integer overflow exists in the user data import/export function of NTG (New Telematics Generation) 6 head units. To perform this attack, local access to USB interface of the car is needed. With prepared data, an attacker can cause the User-Data service to fail. The failed service instance will restart automatically.	N/A	More Details
CVE-2023-34404	Mercedes-Benz head-unit NTG6 has Ethernet pins on Base Board to connect module CSB. Attacker can connect to these pins and get access to internal network. As a result, by accessing a specific port an attacker can send call request to all registered services in router and achieve command injection vulnerability.	N/A	More Details
CVE-2025-0422	An authenticated user in the "bestinformed Web" application can execute commands on the underlying server running the application. (Remote Code Execution) For this, the user must be able to create "ScriptVars" with the type „script" and preview them by, for example, creating a new "Info". By default, admin users have those permissions, but with the granular permission system, those permissions may be assigned to other users. An attacker is able to execute commands on the server running the "bestinformed Web" application if an account with the correct permissions was compromised before.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2025-0423	In the "bestinformed Web" application, some user input was not properly sanitized. This leads to multiple unauthenticated stored cross-site scripting vulnerabilities. An unauthenticated attacker is able to compromise the sessions of users on the server by injecting JavaScript code into their session using an "Unauthenticated Stored Cross-Site Scripting". The attacker is then able to ride the session of those users and can abuse their privileges on the "bestinformed Web" application.	N/A	More Details
CVE-2025-0424	In the "bestinformed Web" application, some user input was not properly sanitized. This leads to multiple authenticated stored cross-site scripting vulnerabilities. An authenticated attacker is able to compromise the sessions of other users on the server by injecting JavaScript code into their session using an "Authenticated Stored Cross-Site Scripting". Those other users might have more privileges than the attacker, enabling a form of horizontal movement.	N/A	More Details
CVE-2025-0425	Via the GUI of the "bestinformed Infoclient", a low-privileged user is by default able to change the server address of the "bestinformed Server" to which this client connects. This is dangerous as the "bestinformed Infoclient" runs with elevated permissions ("nt authority\system"). By changing the server address to a malicious server, or a script simulating a server, the user is able to escalate his privileges by abusing certain features of the "bestinformed Web" server. Those features include: * Pushing of malicious update packages * Arbitrary Registry Read as "nt authority\system" An attacker is able to escalate his privileges to "nt authority\system" on the Windows client running the "bestinformed Infoclient". This attack is not possible if a custom configuration ("Infoclient.ini") containing the flags "ShowOnTaskbar=false" or "DisabledItems=stPort,stAddress" is deployed.	N/A	More Details
CVE-2023-34403	Mercedes-Benz head-unit NTG6 has Ethernet pins on Base Board to connect module CSB. Attacker can connect to this pins and get access to internal network. A race condition can be acquired and attacker can spoof "UserData" with desirable file path and access it though backup on USB.	N/A	More Details
CVE-2020-3432	A vulnerability in the uninstaller component of Cisco AnyConnect Secure Mobility Client for Mac OS could allow an authenticated, local attacker to corrupt the content of any file in the filesystem. The vulnerability is due to the incorrect handling of directory paths. An attacker could exploit this vulnerability by creating a symbolic link (symlink) to a target file on a specific path. A successful exploit could allow the attacker to corrupt the contents of the file. If the file is a critical systems file, the exploit could lead to a denial of service condition. To exploit this vulnerability, the attacker would need to have valid credentials on the system.	N/A	More Details