SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 November 2025

Generated on 05 November 2025

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-29270	Incorrect access control in the realtime.cgi endpoint of Deep Sea Electronics devices DSE855 v1.1.0 to v1.1.26 allows attackers to gain access to the admin panel and complete control of the device.	10.0	More Details
CVE-2025-52665	A malicious actor with access to the management network could exploit a misconfiguration in UniFi's door access application, UniFi Access, that exposed a management API without proper authentication. This vulnerability was introduced in Version 3.3.22 and was fixed in Version 4.0.21 and later. Affected Products: UniFi Access Application (Version 3.3.22 through 3.4.31). Mitigation: Update your UniFi Access Application to Version 4.0.21 or later.	10.0	More Details
CVE-2025-61945	Radiometrics VizAir is vulnerable to any remote attacker via access to the admin panel of the VizAir system without authentication. Once inside, the attacker can modify critical weather parameters such as wind shear alerts, inversion depth, and CAPE values, which are essential for accurate weather forecasting and flight safety. This unauthorized access could result in the disabling of vital alerts, causing hazardous conditions for aircraft, and manipulating runway assignments, which could result in mid-air conflicts or runway incursions.	10.0	More Details
CVE-2025-54863	Radiometrics VizAir is vulnerable to exposure of the system's REST API key through a publicly accessible configuration file. This allows attackers to remotely alter weather data and configurations, automate attacks against multiple instances, and extract sensitive meteorological data, which could potentially compromise airport operations. Additionally, attackers could flood the system with false alerts, leading to a denial-of-service condition and significant disruption to airport operations. Unauthorized remote control over aviation weather monitoring and data manipulation could result in incorrect flight planning and hazardous takeoff and landing conditions.	10.0	More Details
CVE-2025-61956	Radiometrics VizAir is vulnerable to a lack of authentication mechanisms for critical functions, such as admin access and API requests. Attackers can modify configurations without authentication, potentially manipulating active runway settings and misleading air traffic control (ATC) and pilots. Additionally, manipulated meteorological data could mislead forecasters and ATC, causing inaccurate flight planning.	10.0	More Details
CVE-2025-0987	Authorization Bypass Through User-Controlled Key vulnerability in CB Project Ltd. Co. CVLand allows Parameter Injection.This issue affects CVLand: from 2.1.0 through 20251103.	9.9	More Details
	A vulnerability was identified in NeuVector, where the enforcer used environment variables CLUSTER_RPC_PORT and CLUSTER_LAN_PORT to generate a command to be executed via popen, without first sanitising their values. The entry process of the enforcer container is the monitor process. When the enforcer container stops, the monitor process checks whether the consul subprocess has		

CVE-2025-54469	exited. To perform this check, the monitor process uses the popen function to execute a shell command that determines whether the ports used by the consul subprocess are still active. The values of environment variables CLUSTER_RPC_PORT and CLUSTER_LAN_PORT are used directly to compose shell commands via popen without validation or sanitization. This behavior could allow a malicious user to inject malicious commands through these variables within the enforcer container.	9.9	More Details
CVE-2025-48983	A vulnerability in the Mount service of Veeam Backup & Replication, which allows for remote code execution (RCE) on the Backup infrastructure hosts by an authenticated domain user.	9.9	More Details
CVE-2025-8900	The Doccure Core plugin for WordPress is vulnerable to privilege escalation in versions up to, and excluding, 1.5.4. This is due to the plugin allowing users who are registering new accounts to set their own role or by supplying 'user_type' field. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role.	9.8	More Details
CVE-2025-63622	A vulnerability was found in code-projects Online Complaint Site 1.0. This issue affects some unknown processing of the file /cms/admin/subcategory.php. This manipulation of the argument category causes SQL injection.	9.8	More Details
CVE-2025-64102	Zitadel is open-source identity infrastructure software. Prior to 4.6.0, 3.4.3, and 2.71.18, an attacker can perform an online brute-force attack on OTP, TOTP, and passwords. While Zitadel allows preventing online brute force attacks in scenarios like TOTP, Email OTP, or passwords using a lockout mechanism. The mechanism is not enabled by default and can cause a denial of service for the corresponding user if enabled. Additionally, the mitigation strategies were not fully implemented in the more recent resource-based APIs. This vulnerability is fixed in 4.6.0, 3.4.3, and 2.71.18.	9.8	More Details
CVE-2025-12682	The Easy Upload Files During Checkout plugin for WordPress is vulnerable to arbitrary JavaScript file uploads due to missing file type validation in the 'file_during_checkout' function in all versions up to, and including, 2.9.8. This makes it possible for unauthenticated attackers to upload arbitrary JavaScript files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-12493	The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +21 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.5 via the 'load_template' function. This makes it possible for unauthenticated attackers to include and execute arbitrary .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 file types can be uploaded and included.	9.8	More Details
CVE-2025-12158	The Simple User Capabilities plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the suc_submit_capabilities() function in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to elevate the role of any user account to administrator.	9.8	More Details
CVE-2025-11008	The CE21 Suite plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.3.1 via the log file. This makes it possible for unauthenticated attackers to extract sensitive data including authentication credentials, which can be used to log in as other users as long as they have used the plugin's custom authentication feature before. This may include administrators, which makes a complete site takeover possible.	9.8	More Details
CVE-2025-11007	The CE21 Suite plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the wp_ajax_nopriv_ce21_single_sign_on_save_api_settings AJAX action in versions 2.2.1 to 2.3.1. This makes it possible for unauthenticated attackers to update the plugin's API settings including a secret key used for authentication. This allows unauthenticated attackers to create new admin accounts on an affected site.	9.8	More Details
CVE-2025-12463	An unauthenticated SQL Injection was discovered within the Geutebruck G-Cam E-Series Cameras through the `Group` parameter in the `/uapi-cgi/viewer/Param.cgi` script. This has been confirmed on the EFD-2130 camera running firmware version 1.12.0.19.	9.8	More Details
CVE-2025-11953	The Metro Development Server, which is opened by the React Native Community CLI, binds to external interfaces by default. The server exposes an endpoint that is vulnerable to OS command injection. This allows unauthenticated network attackers to send a POST request to the server and run arbitrary executables. On Windows, the attackers can also execute arbitrary shell commands with fully controlled arguments.	9.8	More Details
CVE-2025-63453	Car-Booking-System-PHP v.1.0 is vulnerable to SQL Injection in /carlux/contact.php.	9.8	More Details
CVE-2025-63451	Car-Booking-System-PHP v.1.0 is vulnerable to SQL Injection in /carlux/sign-in.php.	9.8	More Details
CVE-2025-11200	MLflow Weak Password Requirements Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of MLflow. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. The issue	9.8	More Details

	results from weak password requirements. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-26916.		
CVE-2025-11201	MLflow Tracking Server Model Creation Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of MLflow Tracking Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of model file paths. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-26921.	9.8	More Details
CVE-2025-11499	The Tablesome Table – Contact Form DB – WPForms, CF7, Gravity, Forminator, Fluent plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image_from_external_url() function in all versions up to, and including, 1.1.32. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible in configurations where unauthenticated users have been provided with a method for adding featured images, and the workflow trigger is created.	9.8	More Details
CVE-2025-11833	The Post SMTP – Complete SMTP Solution with Logs, Alerts, Backup SMTP & Mobile App plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the __construct function in all versions up to, and including, 3.6.0. This makes it possible for unauthenticated attackers to read arbitrary logged emails sent through the Post SMTP plugin, including password reset emails containing password reset links, which can lead to account takeover.	9.8	More Details
CVE-2024-45162	A stack-based buffer overflow issue was discovered in the phddns client in Blu-Castle BCUM221E 1.0.0P220507 via the password field.	9.8	More Details
CVE-2025-57108	Kitware VTK (Visualization Toolkit) through 9.5.0 contains a heap use-after-free vulnerability in vtkGLTFDocumentLoader. The vulnerability manifests during mesh object copy operations where vector members are accessed after the underlying memory has been freed, specifically when handling GLTF files with corrupted or invalid mesh reference structures.	9.8	More Details
CVE-2025-6520	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Abis Technology BAPSIS allows Blind SQL Injection.This issue affects BAPSIS: before 202510271606.	9.8	More Details
CVE-2025-8489	The King Addons for Elementor – Free Elements, Widgets, Templates, and Features for Elementor plugin for WordPress is vulnerable to privilege escalation in versions 24.12.92 to 51.1.14 . This is due to the plugin not properly restricting the roles that users can register with. This makes it possible for unauthenticated attackers to register with administrator-level user accounts.	9.8	More Details
CVE-2025-5397	The Noo JobMonster theme for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 4.8.1. This is due to the check_login() function not properly verifying a user's identity prior to successfully authenticating them This makes it possible for unauthenticated attackers to bypass standard authentication and access administrative user accounts. Please note social login needs to be enabled in order for a site to be impacted by this vulnerability.	9.8	More Details
CVE-2025-64103	Starting from 2.53.6, 2.54.3, and 2.55.0, Zitadel only required multi factor authentication in case the login policy has either enabled requireMFA or requireMFAForLocalUsers. If a user has set up MFA without this requirement, Zitadel would consider single factor auhtenticated sessions as valid as well and not require multiple factors. Bypassing second authentication factors weakens multifactor authentication and enables attackers to bypass the more secure factor. An attacker can target the TOTP code alone, only six digits, bypassing password verification entirely and potentially compromising accounts with 2FA enabled. This vulnerability is fixed in 4.6.0, 3.4.3, and 2.71.18.	9.8	More Details
CVE-2025-43027	A critical severity vulnerability has been identified in the ALPR Manager role of Security Center that could allow attackers to gain administrative access to the Genetec Security Center system. The Genetec engineering team discovered this issue internally. There is currently no evidence that this vulnerability has been exploited in the wild.	9.8	More Details
CVE-2025-50739	iib0011 omni-tools v0.4.0 is vulnerable to remote code execution via unsafe JSON deserialization.	9.8	More Details
CVE-2025-62712	JumpServer is an open source bastion host and an operation and maintenance security audit system. In JumpServer versions prior to v3.10.20-lts and v4.10.11-lts, an authenticated, non-privileged user can retrieve connection tokens belonging to other users via the super-connection API endpoint (/api/v1/authentication/super-connection-token/). When accessed from a web browser, this endpoint returns connection tokens created by all users instead of restricting results to tokens owned by or authorized for the requester. An attacker who obtains these tokens can use them to initiate connections to managed assets on behalf of the original token owners, resulting in unauthorized access and privilege escalation across sensitive systems. This vulnerability is fixed in v3.10.20-lts and v4.10.11-lts.	9.6	More Details
	WordPress plugin Contact Form CFDB7 versions up to and including 1.3.2 are affected by a pre-authentication SQL injection vulnerability that cascades into insecure deserialization (PHP Object Injection). The weakness arises due to insufficient validation of user input in plugin endpoints, allowing		

CVE-2025-4665	crafted input to influence backend queries in unexpected ways. Using specially crafted payloads, this can escalate into unsafe deserialization, enabling arbitrary object injection in PHP. Although the issue is remotely exploitable without authentication, it does require a crafted interaction with the affected endpoint in order to trigger successfully.	9.6	More Details
CVE-2025-63452	Car-Booking-System-PHP v.1.0 is vulnerable to SQL Injection in /carlux/forgot-pass.php.	9.4	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-64108	Cursor is a code editor built for programming with AI. In versions 1.7.44 and below, various NTFS path quirks allow a prompt injection attacker to circumvent sensitive file protections and overwrite files which Cursor requires human approval to overwrite. Modification of some of the protected files can lead to RCE. Must be chained with a prompt injection or malicious model attach. Only affects systems supporting NTFS. This issue is fixed in version 2.0.	8.8	More Details
CVE-2025-36367	IBM i 7.6, 7.5, 7.4, 7.3, and 7.2 is vulnerable to privilege escalation caused by an invalid IBM i SQL services authorization check. A malicious actor can use the elevated privileges of another user profile to gain root access to the host operating system.	8.8	More Details
CVE-2025-43433	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-10896	Multiple plugins for WordPress with the Jewel Theme Recommended Plugins Library are vulnerable to Unrestricted Upload of File with Dangerous Type via arbitrary plugin installation in all versions up to, and including, 1.0.2.3. This is due to missing capability checks on the '*_recommended_upgrade_plugin' function which allows arbitrary plugin URLs to be installed. This makes it possible for authenticated attackers with subscriber-level access and above to upload arbitrary plugin packages to the affected site's server via a crafted plugin URL, which may make remote code execution possible.	8.8	More Details
CVE-2025-43431	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-11724	The EM Beer Manager plugin for WordPress is vulnerable to arbitrary file upload leading to remote code execution in all versions up to, and including, 3.2.3. This is due to missing file type validation in the EMBM_Admin_Untappd_Import_image() function and missing authorization checks on the wp_ajax_embm-untappd-import action. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files including PHP files and execute code on the server granted they can provide a mock HTTP server that responds with specific JSON data.	8.8	More Details
CVE-2025-43419	The issue was addressed with improved memory handling. This issue is fixed in Safari 26, tvOS 26, watchOS 26, iOS 26 and iPadOS 26, visionOS 26. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-64140	Jenkins Azure CLI Plugin 0.9 and earlier does not restrict which commands it executes on the Jenkins controller, allowing attackers with Item/Configure permission to execute arbitrary shell commands.	8.8	More Details
CVE-2025-60785	A remote code execution (RCE) vulnerability in the Postgres Drivers component of iceScrum v7.54 Pro On-prem allows attackers to execute arbitrary code via a crafted HTML page.	8.8	More Details
CVE-2025-61429	An issue in NCR Atleos Terminal Manager (ConfigApp) v3.4.0 allows attackers to escalate privileges via a crafted request.	8.8	More Details
CVE-2025-12622	A vulnerability was determined in Tenda AC10 16.03.10.13. Affected by this vulnerability is the function formSysRunCmd of the file /goform/SysRunCmd. This manipulation of the argument getui causes buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2025-12619	A vulnerability was found in Tenda A15 15.13.07.13. Affected is the function fromSetWirelessRepeat of the file /goform/openNetworkGateway. The manipulation of the argument wpapsk_crypto2_4g results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-	A vulnerability has been found in Tenda AC8 16.03.34.06. This impacts an unknown function of the file /goform/DatabaseIniSet. The manipulation of the argument Time leads to buffer overflow. The attack can be	8.8	More

12618	initiated remotely. The exploit has been disclosed to the public and may be used.		Details
CVE-2025-12611	A vulnerability was identified in Tenda AC21 16.03.08.16. This vulnerability affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg. The manipulation of the argument startIp leads to buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-12596	A security vulnerability has been detected in Tenda AC23 16.03.07.52. Affected is the function saveParentControlInfo of the file /goform/saveParentControlInfo. Such manipulation of the argument Time leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-12595	A weakness has been identified in Tenda AC23 16.03.07.52. This impacts the function formSetVirtualSer of the file /goform/SetVirtualServerCfg. This manipulation of the argument list causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-6990	The kallyas theme for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.24.0 via the `TH_PhpCode` pagebuilder widget. This is due to the theme not restricting access to the code editor widget for non-administrators. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.	8.8	More Details
CVE-2025-27074	Memory corruption while processing a GP command response.	8.8	More Details
CVE-2025-6574	The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and excluding, 6.1. 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-2025-12171	The RESTful Content Syndication plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ingest_image() function in versions 1.1.0 to 1.5.0. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. This requires the attacker have access to a defined third-party server as specified in the settings, so it is unlikely that this will be exploitable by contributor-level users, and more likely to be exploited by administrators who also have access to the plugin's settings.	8.8	More Details
CVE-2025-11755	The WP Delicious – Recipe Plugin for Food Bloggers (formerly Delicious Recipes) plugin for WordPress is vulnerable to arbitrary file uploads when importing recipes via CSV in all versions up to, and including, 1.9.0. This flaw allows an attacker with at least Contributor-level permissions to upload a malicious PHP file by providing a remote URL during a recipe import process, leading to Remote Code Execution (RCE).	8.8	More Details
CVE-2025-5949	The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's identity prior to processing a password change request. This makes it possible for authenticated attackers with subscriber access or higher to reset other users' passwords, including those of admins.	8.8	More Details
CVE-2025-11920	The WPCOM Member plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.7.14 via the action parameter in one of its shortcodes. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary .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 file types can be uploaded and included.	8.8	More Details
CVE-2025-64349	ELOG allows an authenticated user to modify another user's profile. An attacker can edit a target user's email address, then request a password reset, and take control of the target account. By default, ELOG is not configured to allow self-registration.	8.8	More Details
CVE-2025-12507	The service Bizerba Communication Server (BCS) has an unquoted service path. Due to the way Windows searches the executable for the BCS service, malicious programs can be executed.	8.8	More Details
CVE-2025-64353	Deserialization of Untrusted Data vulnerability in Chouby Polylang polylang allows Object Injection.This issue affects Polylang: from n/a through <= 3.7.3.	8.8	More Details
CVE-2025-7846	The WordPress User Extra Fields plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the save_fields() function in all versions up to, and including, 16.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.8	More Details

CVE-2025-48984	A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user.	8.8	More Details
CVE-2025-62726	n8n is an open source workflow automation platform. Prior to 1.113.0, a remote code execution vulnerability exists in the Git Node component available in both Cloud and Self-Hosted versions of n8n. When a malicious actor clones a remote repository containing a pre-commit hook, the subsequent use of the Commit operation in the Git Node can inadvertently trigger the hook's execution. This allows attackers to execute arbitrary code within the n8n environment, potentially compromising the system and any connected credentials or workflows. This vulnerability is fixed in 1.113.0.	8.8	More Details
CVE-2025-61196	An issue in BusinessNext CRMnext v.10.8.3.0 allows a remote attacker to execute arbitrary code via the comments input parameter.	8.8	More Details
CVE-2025-64106	Cursor is a code editor built for programming with AI. In versions 1.7.28 and below, an input validation flaw in Cursor's MCP server installation enables specially crafted deep-links to bypass the standard security warnings and conceal executed commands from users if they choose to accept the server. If an attacker is able to convince a victim to navigate to a malicious deeplink, the victim will not see the correct speedbump modal, and if they choose to accept, will execute commands specified by the attackers deeplink.	8.8	More Details
CVE-2025-64107	Cursor is a code editor built for programming with AI. In versions 1.7.52 and below, manipulating internal settings may lead to RCE. Cursor detects path manipulation via forward slashes (./.cursor/./../../mcp.json etc.), and requires human approval to complete the operation. However, the same kind of manipulation using backslashes was not correctly detected, allowing an attacker who had already achieved prompt injection or some other level of control to overwrite sensitive editor files without approval on Windows machines. This issue is fixed in version 2.0.	8.8	More Details
CVE-2025-43505	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in Xcode 26.1. Processing a maliciously crafted file may lead to heap corruption.	8.8	More Details
CVE-2025-60503	A cross-site scripting (XSS) vulnerability exists in the administrative interface of ultimatefosters UltimatePOS 4.8 where input submitted in the purchase functionality is reflected without proper escaping in the admin log panel page in the 'reference No.' field. This flaw allows an authenticated attacker to execute arbitrary JavaScript in the context of an administrator's browser session, which could lead to session hijacking or other malicious actions.	8.7	More Details
CVE-2025-10897	The WooCommerce Designer Pro theme for WordPress is vulnerable to arbitrary file read in all versions up to, and including, 1.9.28. This makes it possible for unauthenticated attackers to read arbitrary files on the server, which can expose DB credentials when the wp-config.php file is read.	8.6	More Details
CVE-2025-54470	This vulnerability affects NeuVector deployments only when the Report anonymous cluster data option is enabled. When this option is enabled, NeuVector sends anonymous telemetry data to the telemetry server. In affected versions, NeuVector does not enforce TLS certificate verification when transmitting anonymous cluster data to the telemetry server. As a result, the communication channel is susceptible to man-in-the-middle (MITM) attacks, where an attacker could intercept or modify the transmitted data. Additionally, NeuVector loads the response of the telemetry server is loaded into memory without size limitation, which makes it vulnerable to a Denial of Service(DoS) attack	8.6	More Details
CVE-2025-3356	IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 21 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view, overwrite, or append to arbitrary files on the system.	8.6	More Details
CVE-2025-11690	An Insecure Direct Object Reference (IDOR) vulnerability exists in the vehicleId parameter, allowing unauthorized access to sensitive information of other users' vehicles. Exploiting this issue enables an attacker to retrieve data such as GPS coordinates, encryption keys, initialization vectors, model numbers, and fuel statistics belonging to other users, instead of being limited to their own vehicle data. This is a server-side authorization fix.	8.5	More Details
CVE-2025-11702	GitLab has remediated an issue in EE affecting all versions from 17.1 before 18.3.5, 18.4 before 18.4.3, and 18.5 before 18.5.1 that could have allowed an authenticated attacker with specific permissions to hijack project runners from other projects.	8.5	More Details
CVE-2025-12508	When using domain users as BRAIN2 users, communication with Active Directory services is unencrypted. This can lead to the interception of authentication data and compromise confidentiality.	8.4	More Details
CVE-2025-61161	DLL hijacking vulnerability in Evope Collector 1.1.6.9.0 and related components load the wtsapi32.dll library from an uncontrolled search path (C:\ProgramData\Evope). This allows local unprivileged attackers to execute arbitrary code or escalate privileges to SYSTEM by placing a crafted DLL in that location. The vulnerable component is Evope.Service.exe, which runs with SYSTEM privileges and automatically loads the DLL on startup or reboot.	8.4	More Details

CVE-2025-12509	On a client with an admin user, a Global_Shipping script can be implemented. The script could later be executed on the BRAIN2 server with administrator rights.	8.4	More Details
CVE-2025-48396	Arbitrary code execution is possible due to improper validation of the file upload functionality in Eaton BLSS. This security issue has been fixed in the latest script patch latest version of of Eaton BLSS (7.3.0.SCP004).	8.3	More Details
CVE-2025-12357	By manipulating the Signal Level Attenuation Characterization (SLAC) protocol with spoofed measurements, an attacker can stage a man-in-the-middle attack between an electric vehicle and chargers that comply with the ISO 15118-2 part. This vulnerability may be exploitable wirelessly, within close proximity, via electromagnetic induction.	8.3	More Details
CVE-2025-60595	SPH Engineering UgCS 5.13.0 is vulnerable to Arbitary code execution.	8.2	More Details
CVE-2025-23358	NVIDIA NVApp for Windows contains a vulnerability in the installer, where a local attacker can cause a search path element issue. A successful exploit of this vulnerability might lead to code execution and escalation of privileges.	8.2	More Details
CVE-2025-10932	Uncontrolled Resource Consumption vulnerability in Progress MOVEit Transfer (AS2 module).This issue affects MOVEit Transfer: from 2025.0.0 before 2025.0.3, from 2024.1.0 before 2024.1.7, from 2023.1.0 before 2023.1.16.	8.2	More Details
CVE-2025-63298	A path traversal vulnerability was identified in SourceCodester Pet Grooming Management System 1.0, affecting the admin/manage_website.php component. An authenticated user with administrative privileges can leverage this flaw by submitting a specially crafted POST request, enabling the deletion of arbitrary files on the web server or underlying operating system.	8.2	More Details
CVE-2025-43323	This issue was addressed with additional entitlement checks. This issue is fixed in visionOS 26, tvOS 26, iOS 26 and iPadOS 26, watchOS 26. An app may be able to fingerprint the user.	8.1	More Details
CVE-2025-43480	The issue was addressed with improved checks. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. A malicious website may exfiltrate data cross-origin.	8.1	More Details
CVE-2025-64101	Zitadel is open-source identity infrastructure software. Prior to 4.6.0, 3.4.3, and 2.71.18, a potential vulnerability exists in ZITADEL's password reset mechanism. ZITADEL utilizes the Forwarded or X-Forwarded-Host header from incoming requests to construct the URL for the password reset confirmation link. This link, containing a secret code, is then emailed to the user. If an attacker can manipulate these headers (e.g., via host header injection), they could cause ZITADEL to generate a password reset link pointing to a malicious domain controlled by the attacker. If the user clicks this manipulated link in the email, the secret reset code embedded in the URL can be captured by the attacker. This captured code could then be used to reset the user's password and gain unauthorized access to their account. It's important to note that this specific attack vector is mitigated for accounts that have Multi-Factor Authentication (MFA) or Passwordless authentication enabled. This vulnerability is fixed in 4.6.0, 3.4.3, and 2.71.18.	8.1	More Details
CVE-2025-62786	Wazuh is a free and open source platform used for threat prevention, detection, and response. A heap-based out-of-bounds WRITE occurs in decode_win_permissions, resulting in writing a NULL byte 2 bytes before the start of the buffer allocated to decoded_it. A compromised agent can potentially leverage this issue to perform remote code execution, by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can leverage this issue to potentially achieve remote code execution on the wazuh manager (the exploitability of this vulnerability depends on the specifics of the respective heap allocator). This vulnerability is fixed in 4.10.2.	8.1	More Details
CVE-2025-47357	Information Disclosure when a user-level driver performs QFPROM read or write operations on Fuse regions.	8.0	More Details
CVE-2025-64112	Statmatic is a Laravel and Git powered content management system (CMS). Stored XSS vulnerabilities in Collections and Taxonomies allow authenticated users with content creation permissions to inject malicious JavaScript that executes when viewed by higher-privileged users. This vulnerability is fixed in 5.22.1.	8.0	More Details
CVE-2025-62618	ELOG allows an authenticated user to upload arbitrary HTML files. The HTML content is executed in the context of other users when they open the file. Because ELOG includes usernames and password hashes in certain HTTP requests, an attacker can obtain the target's credentials and replay them or crack the password hash offline. In ELOG 3.1.5-20251014 release, HTML files are rendered as plain text.	8.0	More Details
CVE-2025-	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User	8.0	More Details

20742	interaction is not needed for exploitation. Patch ID: WCNCR00432680; Issue ID: MSV-3949.		
CVE-2025-20728	In wlan STA driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00447115; Issue ID: MSV-4276.	7.8	More Details
CVE-2025-20733	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00441509; Issue ID: MSV-4138.	7.8	More Details
CVE-2025-43940	Dell Unity, version(s) 5.5 and Prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution and Elevation of privileges.	7.8	More Details
CVE-2025-43942	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution and Elevation of privileges.	7.8	More Details
CVE-2025-61156	Incorrect access control in the kernel driver of ThreatFire System Monitor v4.7.0.53 allows attackers to escalate privileges and execute arbitrary commands via an insecure IOCTL.	7.8	More Details
CVE-2025-20735	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00435349; Issue ID: MSV-4051.	7.8	More Details
CVE-2025-20737	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00435343; Issue ID: MSV-4040.	7.8	More Details
CVE-2025-54496	A maliciously crafted project file may cause a heap-based buffer overflow in Fuji Electric Monitouch V-SFT-6, which may allow the attacker to execute arbitrary code.	7.8	More Details
CVE-2025-54526	Fuji Electric Monitouch V-SFT-6 is vulnerable to a stack-based buffer overflow while processing a specially crafted project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2025-46422	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	7.8	More Details
CVE-2025-46423	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	7.8	More Details
CVE-2025-47360	Memory corruption while processing client message during device management.	7.8	More Details
CVE-2025-54545	On affected platforms, a restricted user could break out of the CLI sandbox to the system shell and elevate their privileges.	7.8	More Details
CVE-2025-57227	An unquoted service path in Kingosoft Technology Ltd Kingo ROOT v1.5.8.3353 allows attackers to escalate privileges via placing a crafted executable file into a parent folder.	7.8	More Details
CVE-2025-60749	DLL Hijacking vulnerability in Trimble SketchUp desktop 2025 via crafted libcef.dll used by sketchup_webhelper.exe.	7.8	More Details
CVE-2025-11463	Ashlar-Vellum Cobalt XE File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XE files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26626.	7.8	More Details
CVE-2025-	Ashlar-Vellum Cobalt CO File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack	7.8	More

11464	of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26628.		Details
CVE-2025-11465	Ashlar-Vellum Cobalt CO File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ashlar-Vellum Cobalt. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CO files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26631.	7.8	More Details
CVE-2025-33003	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 could allow a non-root user to gain higher privileges/capabilities within the scope of a container due to execution with unnecessary privileges.	7.8	More Details
CVE-2025-47361	Memory corruption when triggering a subsystem crash with an out-of-range identifier.	7.8	More Details
CVE-2025-43939	Dell Unity, version(s) 5.4 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution and Elevation of privileges.	7.8	More Details
CVE-2025-43407	This issue was addressed with improved entitlements. This issue is fixed in visionOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, iOS 26.1 and iPadOS 26.1, tvOS 26.1. An app may be able to break out of its sandbox.	7.8	More Details
CVE-2025-43361	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 26, watchOS 26, iOS 26 and iPadOS 26, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, visionOS 26. A malicious app may be able to read kernel memory.	7.8	More Details
CVE-2025-43474	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to cause unexpected system termination or read kernel memory.	7.8	More Details
CVE-2025-47367	Memory corruption while accessing a buffer during IOCTL processing.	7.8	More Details
CVE-2025-43472	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to gain root privileges.	7.8	More Details
CVE-2025-47368	Memory corruption when dereferencing an invalid userspace address in a user buffer during MCDM IOCTL processing.	7.8	More Details
CVE-2025-43387	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.2. A malicious app may be able to gain root privileges.	7.8	More Details
CVE-2025-43476	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to break out of its sandbox.	7.8	More Details
CVE-2025-27070	Memory corruption while performing encryption and decryption commands.	7.8	More Details
CVE-2025-47365	Memory corruption while processing large input data from a remote source via a communication interface.	7.8	More Details
CVE-2025-47353	Memory corruption while processing request sent from GVM.	7.8	More Details
CVE-2025-47352	Memory corruption while processing audio streaming operations.	7.8	More Details
CVE-2025-	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.8, macOS Sequoia 15.7. An app may be able to break out of its sandbox.	7.8	More Details

43364			
CVE-2025-64366	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stylemix MasterStudy LMS masterstudy-lms-learning-management-system allows Blind SQL Injection.This issue affects MasterStudy LMS: from n/a through <= 3.6.27.	7.6	More Details
CVE-2025-64360	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in StylemixThemes Consulting Elementor Widgets consulting-elementor-widgets allows PHP Local File Inclusion.This issue affects Consulting Elementor Widgets: from n/a through <= 1.4.2.	7.5	More Details
CVE-2025-64364	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in StylemixThemes Masterstudy masterstudy allows PHP Local File Inclusion.This issue affects Masterstudy: from n/a through < 4.8.126.	7.5	More Details
CVE-2025-64359	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in StylemixThemes Consulting consulting allows PHP Local File Inclusion.This issue affects Consulting: from n/a through < 6.7.5.	7.5	More Details
CVE-2024-56426	An issue was discovered in Samsung Mobile Processor and Wearable Processor Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, W920, W930, W1000. The lack of a length check leads to out-of-bounds writes via malformed USB packets to the target.	7.5	More Details
CVE-2025-58149	When passing through PCI devices, the detach logic in libxl won't remove access permissions to any 64bit memory BARs the device might have. As a result a domain can still have access any 64bit memory BAR when such device is no longer assigned to the domain. For PV domains the permission leak allows the domain itself to map the memory in the page-tables. For HVM it would require a compromised device model or stubdomain to map the leaked memory into the HVM domain p2m.	7.5	More Details
CVE-2025-12501	Integer overflow in GameMaker IDE below 2024.14.0 version can lead to can lead to application crashes through denial-of-service attacks (DoS). GameMaker users who use the network_create_server() function in their projects are urged to update and recompile immediately.	7.5	More Details
CVE-2025-58148	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Some Viridian hypercalls can specify a mask of vCPU IDs as an input, in one of three formats. Xen has boundary checking bugs with all three formats, which can cause out-of-bounds reads and writes while processing the inputs. * CVE-2025-58147. Hypercalls using the HV_VP_SET Sparse format can cause vpmask_set() to write out of bounds when converting the bitmap to Xen's format. * CVE-2025-58148. Hypercalls using any input format can cause send_ipi() to read d->vcpu[] out-of-bounds, and operate on a wild vCPU pointer.	7.5	More Details
CVE-2025-58147	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Some Viridian hypercalls can specify a mask of vCPU IDs as an input, in one of three formats. Xen has boundary checking bugs with all three formats, which can cause out-of-bounds reads and writes while processing the inputs. * CVE-2025-58147. Hypercalls using the HV_VP_SET Sparse format can cause vpmask_set() to write out of bounds when converting the bitmap to Xen's format. * CVE-2025-58148. Hypercalls using any input format can cause send_ipi() to read d->vcpu[] out-of-bounds, and operate on a wild vCPU pointer.	7.5	More Details
CVE-2025-12115	The WPC Name Your Price for WooCommerce plugin for WordPress is vulnerable to unauthorized price alteration in all versions up to, and including, 2.1.9. This is due to the plugin not disabling the ability to name a custom price when it has been specifically disabled for a product. This makes it possible for unauthenticated attackers to purchase products at prices less than they should be able to.	7.5	More Details
CVE-2025-62232	Sensitive data exposure via logging in basic-auth leads to plaintext usernames and passwords written to error logs and forwarded to log sinks when log level is INFO/DEBUG. This creates a high risk of credential compromise through log access. It has been fixed in the following commit: https://github.com/apache/apisix/pull/12629 Users are recommended to upgrade to version 3.14, which fixes this issue.	7.5	More Details
CVE-2025-30188	Malicious or unintentional API requests can be used to add significant amount of data to caches. Caches may evict information that is required to operate the web frontend, which leads to unavailability of the component. Please deploy the provided updates and patch releases. No publicly available exploits are known	7.5	More Details
CVE-2025-43469	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	7.5	More Details
CVE-2025-32786	The GLPI Inventory Plugin handles network discovery, inventory, software deployment, and data collection for GLPI agents. Versions 1.5.0 and below are vulnerable to SQL Injection. This issue is fixed in version 1.5.1.	7.5	More Details
CVE-2025-	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.1 and iPadOS 26.1. An attacker may be able to view restricted content from the lock screen.	7.5	More Details

43350			
CVE-2025-43496	The issue was addressed by adding additional logic. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, macOS Sequoia 15.7.2, visionOS 26.1. Remote content may be loaded even when the 'Load Remote Images' setting is turned off.	7.5	More Details
CVE-2025-63423	Each Italy Wireless Mini Router WIRELESS-N 300M v28K.MiniRouter.20190211 was discovered to store the Administrator password.	7.5	More Details
CVE-2025-61120	AG Life Logger Android App version v1.0.2.72 and before (package name com.donki.healthy), developed by IO FIT, K.K., contains improper access control vulnerabilities. Exposed credentials in traffic may allow attackers to misuse cloud resources, and predictable verification codes make brute-force account logins feasible. Successful exploitation could result in account compromise, privacy breaches, and abuse of cloud resources.	7.5	More Details
CVE-2025-61113	TalkTalk 3.3.6 Android App contains improper access control vulnerabilities in multiple API endpoints. By modifying request parameters, attackers may obtain sensitive user information (such as device identifiers and birthdays) and access private group information, including join credentials. Successful exploitation may result in privacy breaches and unauthorized access to restricted resources.	7.5	More Details
CVE-2025-61115	ABC Fine Wine & Spirits Android App version v.11.27.5 and before (package name com.cta.abcfinewineandspirits), developed by ABC Liquors, Inc., contains an improper access control vulnerability in its login mechanism. The application does not properly validate user passwords during authentication, allowing attackers to bypass login checks and obtain valid session identifiers. Successful exploitation could result in unauthorized account access, privacy breaches, and misuse of the platform.	7.5	More Details
CVE-2025-61116	AdForest - Classified Android App version 4.0.12 (package name scriptsbundle.adforest), developed by Muhammad Jawad Arshad, contains an improper access control vulnerability in its authentication mechanism. The app uses a Base64-encoded email address as the authorization credential, which can be manipulated by attackers to gain unauthorized access to user accounts. Successful exploitation could result in account compromise, privacy breaches, and misuse of the platform.	7.5	More Details
CVE-2025-61117	Senza: Keto & Fasting Android App version 2.10.15 (package name com.gl.senza), developed by Paul Itoi, contains an improper access control vulnerability. By exploiting insufficient checks in user data API endpoints, attackers can obtain authentication tokens and perform account takeover. Successful exploitation could result in unauthorized account access, privacy breaches, and misuse of the platform.	7.5	More Details
CVE-2025-61118	mCarFix Motorists App version 2.3 (package name com.skytop.mcarfix), developed by Paniel Mwaura, contains improper access control vulnerabilities. Attackers may bypass verification to arbitrarily register accounts, and by tampering with sequential numeric IDs, gain unauthorized access to user data and groups. Successful exploitation could result in fake account creation, privacy breaches, and misuse of the platform.	7.5	More Details
CVE-2025-61114	2nd Line Android App version v1.2.92 and before (package name com.mysecondline.app), developed by AutoBizLine, Inc., contains an improper access control vulnerability in its authentication mechanism. The server only validates the first character of the user_token, enabling attackers to brute force tokens and perform unauthorized queries on other user accounts. Successful exploitation could result in privacy breaches and unauthorized access to user data.	7.5	More Details
CVE-2025-61119	Kanova Android App version 1.0.27 (package name com.karelane), developed by Karely L.L.C., contains improper access control vulnerabilities. Attackers may gain unauthorized access to user details and obtain group information, including entry codes, by manipulating API request parameters. Successful exploitation could result in privacy breaches, unauthorized group access, and misuse of the platform.	7.5	More Details
CVE-2025-61121	Mobile Scanner Android App version 2.12.38 (package name com.glority.everlens), developed by Glority Global Group Ltd., contains a credential leakage vulnerability. Improper handling of cloud service credentials may allow attackers to obtain them and carry out unauthorized actions, such as sensitive information disclosure and abuse of cloud resources. Successful exploitation could result in privacy breaches and misuse of the platform infrastructure.	7.5	More Details
CVE-2025-61498	A buffer overflow in the UPnP service of Tenda AC8 Hardware v03.03.10.01 allows attackers to cause a Denial of Service (DoS) via supplying a crafted packet.	7.5	More Details
CVE-2025-56230	Tencent Docs Desktop 3.9.20 and earlier suffers from Missing SSL Certificate Validation in the update component.	7.5	More Details
CVE-2025-43502	A privacy issue was addressed by removing sensitive data. This issue is fixed in iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. An app may be able to bypass certain Privacy preferences.	7.5	More Details
CVE-			

2025-43500	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, visionOS 26.1. An app may be able to access sensitive user data.	7.5	More Details
CVE-2025-63422	Incorrect access control in the Web management interface in Each Italy Wireless Mini Router WIRELESS-N 300M v28K.MiniRouter.20190211 allows attackers to arbitrarily change the administrator username and password via sending a crafted GET request.	7.5	More Details
CVE-2025-3355	IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 21 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	7.5	More Details
CVE-2025-43468	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	7.5	More Details
CVE-2025-61141	sqls-server/sqls 0.2.28 is vulnerable to command injection in the config command because the openEditor function passes the EDITOR environment variable and config file path to sh -c without sanitization, allowing attackers to execute arbitrary commands.	7.5	More Details
CVE-2025-57106	Kitware VTK (Visualization Toolkit) up to 9.5.0 is vulnerable to Buffer Overflow in vtkGLTFDocumentLoader. The vulnerability occurs in the BufferDataExtractionWorker template function when processing GLTF accessor data.	7.5	More Details
CVE-2025-43452	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 26.1 and iPadOS 26.1. Keyboard suggestions may display sensitive information on the lock screen.	7.5	More Details
CVE-2025-43462	The issue was addressed with improved memory handling. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1. An app may be able to cause unexpected system termination or corrupt kernel memory.	7.5	More Details
CVE-2025-43405	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access user-sensitive data.	7.5	More Details
CVE-2025-11890	The Crypto Payment Gateway with Payeer for WooCommerce plugin for WordPress is vulnerable to payment bypass in all versions up to, and including, 1.0.3. This is due to the plugin not properly verifying a payments status through server-side validation though the /wc-api/bp-payeer-gateway-callback endpoint. This makes it possible for unauthenticated attackers to update unpaid order statuses to paid resulting in a loss of revenue.	7.5	More Details
CVE-2025-43413	An access issue was addressed with additional sandbox restrictions. This issue is fixed in visionOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. A sandboxed app may be able to observe system-wide network connections.	7.5	More Details
CVE-2025-52513	An issue was discovered in Samsung Mobile Processor Exynos 2400, 1580, 2500. A race condition in the HTS driver results in an out-of-bounds write, leading to a denial of service.	7.5	More Details
CVE-2025-52512	An issue was discovered in Samsung Mobile Processor Exynos 2400, 1580, 2500. A race condition in the HTS driver results in out-of-bounds memory access, leading to a denial of service.	7.5	More Details
CVE-2025-54332	An issue was discovered in NPU in Samsung Mobile Processor Exynos through July 2025. There is a NULL Pointer Dereference of profiler.node in the npu_vertex_profileoff function.	7.5	More Details
CVE-2025-54329	An issue was discovered in NAS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. The function used to send a multiple-payloads message (including an SMS message) lacks bounds checking, which can lead to a heap overflow.	7.5	More Details
CVE-2025-54323	An issue was discovered in the camera in Samsung Mobile Processor Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, and 1580. Improper debug printing leads to information leakage.	7.5	More Details
CVE-2025-43409	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	7.5	More Details
CVE-2025-20725	In ims service, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01671924; Issue ID: MSV-4620.	7.5	More Details

CVE-2025-43424	The issue was addressed with improved bounds checks. This issue is fixed in iOS 26.1 and iPadOS 26.1. A malicious HID device may cause an unexpected process crash.	7.5	More Details
CVE-2025-43401	A denial-of-service issue was addressed with improved validation. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. A remote attacker may be able to cause a denial-of-service.	7.5	More Details
CVE-2025-43399	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15.7.2. An app may be able to access protected user data.	7.5	More Details
CVE-2025-43389	A privacy issue was addressed by removing the vulnerable code. This issue is fixed in iOS 26.1 and iPadOS 26.1, macOS Sequoia 15.7.2, macOS Sonoma 14.8.2, visionOS 26.1. An app may be able to access sensitive user data.	7.5	More Details
CVE-2025-43385	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1, macOS Sequoia 15.7.2. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	7.5	More Details
CVE-2025-20727	In Modem, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01672601; Issue ID: MSV-4623.	7.5	More Details
CVE-2025-43373	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to cause unexpected system termination or corrupt kernel memory.	7.5	More Details
CVE-2025-20726	In Modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01672598; Issue ID: MSV-4622.	7.5	More Details
CVE-2025-50735	Directory traversal vulnerability in NextChat thru 2.16.0 due to the WebDAV proxy failing to canonicalize or reject dot path segments in its catch-all route, allowing attackers to gain sensitive information via authenticated or anonymous WebDAV endpoints.	7.5	More Details
CVE-2025-54334	An issue was discovered in the NPU driver in Samsung Mobile Processor Exynos 1280, 2200, 1380, 1480, 2400, 1580, 2500. There is a NULL Pointer Dereference of hdev in the __npu_vertex_bootup function.	7.5	More Details
CVE-2025-11704	The Elegance Menu plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.9 via the 'elegance-menu' attribute of the `elegance-menu` shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary .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 file types can be uploaded and included.	7.5	More Details
CVE-2025-43454	This issue was addressed through improved state management. This issue is fixed in iOS 26.1 and iPadOS 26.1. A device may persistently fail to lock.	7.5	More Details
CVE-2025-63460	Totolink A7000R v9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the ssid5g parameter in the sub_4222E0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-43450	A logic issue was addressed with improved checks. This issue is fixed in iOS 26.1 and iPadOS 26.1. An app may be able to learn information about the current camera view before being granted camera access.	7.5	More Details
CVE-2025-49494	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem. Mishandling of an 5G NRMM packet leads to a Denial of Service.	7.5	More Details
CVE-2025-43449	The issue was addressed with improved handling of caches. This issue is fixed in iOS 26.1 and iPadOS 26.1. A malicious app may be able to track users between installs.	7.5	More Details
CVE-2025-43442	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.1 and iPadOS 26.1. An app may be able to identify what other apps a user has installed.	7.5	More Details

CVE-2025-63466	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the password parameter in the sub_426EF8 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63467	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the ssid parameter in the sub_425400 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63468	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the http_host parameter in the sub_426EF8 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63469	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the ssid parameter in the sub_421BAC function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-43439	A privacy issue was addressed by removing sensitive data. This issue is fixed in iOS 26.1 and iPadOS 26.1, visionOS 26.1. An app may be able to fingerprint the user.	7.5	More Details
CVE-2025-63458	Tenda AX-1803 v1.0.0.1 was discovered to contain a stack overflow via the timeZone parameter in the form_fast_setting_wifi_set function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63461	Totolink A7000R v9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the ssid5g parameter in the urldecode function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63462	Totolink A7000R v9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the wifiOff parameter in the sub_421A04 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63463	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the wifiOff parameter in the sub_4232EC function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63464	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the ssid parameter in the sub_42396C function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-43436	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1. An app may be able to enumerate a user's installed apps.	7.5	More Details
CVE-2025-63465	Totolink LR350 v9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the ssid parameter in the sub_422880 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63459	Totolink A7000R v9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the ssid5g parameter in the sub_421CF0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63454	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow via the deviceId parameter in the get_parentControl_list_Info function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-63561	Summer Pearl Group Vacation Rental Management Platform prior to 1.0.2 is susceptible to a Slowloris-style Denial-of-Service (DoS) condition in the HTTP connection handling layer, where an attacker that opens and maintains many slow or partially-completed HTTP connections can exhaust the server’s connection pool and worker capacity, preventing legitimate users and APIs from accessing the service.	7.5	More Details
CVE-2025-64363	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in SeventhQueen Kleo kleo allows PHP Local File Inclusion.This issue affects Kleo: from n/a through < 5.5.0.	7.5	More Details
CVE-2025-54459	Prior to September 19, 2025, the Hospital Manager Backend Services exposed the ASP.NET tracing endpoint /trace.axd without authentication, allowing a remote attacker to obtain live request traces and sensitive information such as request metadata, session identifiers, authorization headers, server variables, and internal file paths.	7.5	More Details
CVE-2025-64216	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeSphere SmartMag smart-mag allows PHP Local File Inclusion.This issue affects SmartMag: from n/a through <= 10.3.0.	7.5	More Details

CVE-2025-61725	The ParseAddress function constructeds domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.	7.5	More Details
CVE-2025-64284	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Majestic Support Majestic Support majestic-support allows PHP Local File Inclusion.This issue affects Majestic Support: from n/a through <= 1.1.1.	7.5	More Details
CVE-2025-62787	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to 4.10.2, a buffer over-read occurs in DecodeWinevt() when child_attr[p]->attributes[j] is accessed, because the corresponding index (j) is incorrect. A compromised agent can cause a READ operation beyond the end of the allocated buffer (which may contain sensitive information) by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can cause a buffer over-read and potentially access sensitive data. While the buffer over-read is always triggered while resolving the arguments of mdebug2, specific configuration options (analysisd.debug=2) need to be in place for the respective data to be leaked. This vulnerability is fixed in 4.10.2.	7.5	More Details
CVE-2025-61234	Incorrect access control on Dataphone A920 v2025.07.161103 exposes a service on port 8888 by default on the local network without authentication. This allows an attacker to interact with the device via a TCP socket without credentials. Additionally, sending an HTTP request to the service on port 8888 triggers an error in the response, which exposes the functionality, headers identifying Paytef dataphone packets, and the build version.	7.5	More Details
CVE-2025-61723	The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.	7.5	More Details
CVE-2025-58187	Due to the design of the name constraint checking algorithm, the processing time of some inputs scals non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.	7.5	More Details
CVE-2025-62789	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to 4.11.0, fim_alert() implementation does not check whether the return value of ctime_r is NULL or not before calling strdup() on it. A compromised agent can cause a crash of analysisd by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can cause analysisd to crash and make it unavailable. This vulnerability is fixed in 4.11.0.	7.5	More Details
CVE-2025-58188	Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.	7.5	More Details
CVE-2025-62788	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to 4.11.0, w_copy_event_for_log() references memory (initially allocated in OS_CleanMSG()) after it has been freed. A compromised agent can potentially compromise the integrity of the application by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can leverage this issue to potentially compromise the integrity of the application (the use of previously freed memory may corrupt valid data, if the memory area in question has been allocated and used properly elsewhere). This vulnerability is fixed in 4.11.0.	7.5	More Details
CVE-2025-62790	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to 4.11.0, fim_fetch_attributes_state() implementation does not check whether time_string is NULL or not before calling strlen() on it. A compromised agent can cause a crash of analysisd by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can cause analysisd to crash and make it unavailable. This vulnerability is fixed in 4.11.0.	7.5	More Details
CVE-2025-64195	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThimPress Eduma eduma allows PHP Local File Inclusion.This issue affects Eduma: from n/a through <= 5.7.6.	7.5	More Details
CVE-2025-62785	Wazuh is a free and open source platform used for threat prevention, detection, and response. fillData() implementation does not check whether value is NULL or not before calling os_strdup() on it. A compromised agent can cause a crash of analysisd by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can cause analysisd to crash and make it unavailable. This vulnerability is fixed in 4.10.2.	7.5	More Details
CVE-2025-62791	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to 4.11.0, DecodeCiscat() implementation does not check the return the value of cJSON_GetObjectItem() for a possible NULL value in case of an error. A compromised agent can cause a crash of analysisd by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can cause analysisd to crash and make it unavailable. This vulnerability is fixed in 4.11.0.	7.5	More Details

CVE-2025-56558	An issue discovered in Dyson App v6.1.23041-23595 allows unauthenticated attackers to control other users' Dyson IoT devices remotely via MQTT.	7.5	More Details
CVE-2025-64131	Jenkins SAML Plugin 4.583.vc68232f7018a_ and earlier does not implement a replay cache, allowing attackers able to obtain information about the SAML authentication flow between a user's web browser and Jenkins to replay those requests, authenticating to Jenkins as that user.	7.5	More Details
CVE-2025-12082	Incorrect Authorization vulnerability in Drupal CivicTheme Design System allows Forceful Browsing.This issue affects CivicTheme Design System: from 0.0.0 before 1.12.0.	7.5	More Details
CVE-2025-62792	Wazuh is a free and open source platform used for threat prevention, detection, and response. Prior to 4.12.0, a buffer over-read occurs in w_expression_match() when strlen() is called on str_test, because the corresponding buffer is not being properly NULL terminated during its allocation in OS_CleanMSG(). A compromised agent can cause a READ operation beyond the end of the allocated buffer (which may contain sensitive information) by sending a specially crafted message to the wazuh manager. An attacker who is able to craft and send an agent message to the wazuh manager can cause a buffer over-read and potentially access sensitive data. This vulnerability is fixed in 4.12.0.	7.5	More Details
CVE-2025-12466	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Simple OAuth (OAuth2) & OpenID Connect allows Authentication Bypass.This issue affects Simple OAuth (OAuth2) & OpenID Connect: from 6.0.0 before 6.0.7.	7.5	More Details
CVE-2025-11232	To trigger the issue, three configuration parameters must have specific settings: "hostname-char-set" must be left at the default setting, which is "[^A-Za-z0-9.-]"; "hostname-char-replacement" must be empty (the default); and "ddns-qualifying-suffix" must *NOT* be empty (the default is empty). DDNS updates do not need to be enabled for this issue to manifest. A client that sends certain option content would then cause kea-dhcp4 to exit unexpectedly. This issue affects Kea versions 3.0.1 through 3.0.1 and 3.1.1 through 3.1.2.	7.5	More Details
CVE-2025-9954	Missing Authorization vulnerability in Drupal Acquia DAM allows Forceful Browsing.This issue affects Acquia DAM: from 0.0.0 before 1.1.5.	7.5	More Details
CVE-2025-54546	On affected platforms, restricted users could use SSH port forwarding to access host-internal services	7.5	More Details
CVE-2025-30189	When cache is enabled, some passdb/userdb drivers incorrectly cache all users with same cache key, causing wrong cached information to be used for these users. After cached login, all subsequent logins are for same user. Install fixed version or disable caching either globally or for the impacted passdb/userdb drivers. No publicly available exploits are known.	7.4	More Details
CVE-2025-12617	A flaw has been found in itsourcecode Billing System 1.0. This affects an unknown function of the file /admin/app/login_crud.php. Executing manipulation of the argument Password can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-63441	Open Source Social Network (OSSN) 8.6 is vulnerable to Cross Site Scripting (XSS) via the parameter param` at endpoint u/administrator/friends.	7.3	More Details
CVE-2025-12606	A vulnerability was determined in itsourcecode Online Loan Management System 1.0. This issue affects some unknown processing of the file /manage_borrower.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-62229	A flaw was found in the X.Org X server and Xwayland when processing X11 Present extension notifications. Improper error handling during notification creation can leave dangling pointers that lead to a use-after-free condition. This can cause memory corruption or a crash, potentially allowing an attacker to execute arbitrary code or cause a denial of service.	7.3	More Details
CVE-2025-62230	A flaw was discovered in the X.Org X server's X Keyboard (Xkb) extension when handling client resource cleanup. The software frees certain data structures without properly detaching related resources, leading to a use-after-free condition. This can cause memory corruption or a crash when affected clients disconnect.	7.3	More Details
CVE-2025-12605	A vulnerability was found in itsourcecode Online Loan Management System 1.0. This vulnerability affects unknown code of the file /manage_loan.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-62231	A flaw was identified in the X.Org X server's X Keyboard (Xkb) extension where improper bounds checking in the XkbSetCompatMap() function can cause an unsigned short overflow. If an attacker sends specially crafted input data, the value calculation may overflow, leading to memory corruption or a crash.	7.3	More Details

CVE-2025-12604	A vulnerability has been found in itsourcecode Online Loan Management System 1.0. This affects an unknown part of the file /load_fields.php. The manipulation of the argument loan_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-52663	A vulnerability was identified in certain UniFi Talk devices where internal debugging functionality remained unintentionally enabled. This issue could allow an attacker with access to the UniFi Talk management network to invoke internal debug operations through the device API. Affected Products: UniFi Talk Touch (Version 1.21.16 and earlier) UniFi Talk Touch Max (Version 2.21.22 and earlier) UniFi Talk G3 Phones (Version 3.21.26 and earlier) Mitigation: Update the UniFi Talk Touch to Version 1.21.17 or later. Update the UniFi Talk Touch Max to Version 2.21.23 or later. Update the UniFi Talk G3 Phones to Version 3.21.27 or later.	7.3	More Details
CVE-2025-10487	The Advanced Ads – Ad Manager & AdSense plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.0.12 via the select_one() function. This is due to the endpoint not properly restricting access to the AJAX endpoint or limiting the functions that can be called to safe functions. This makes it possible for unauthenticated attackers to call arbitrary functions beginning with get_the_ like get_the_excerpt which can make information exposure possible.	7.3	More Details
CVE-2025-12607	A vulnerability was identified in itsourcecode Online Loan Management System 1.0. Impacted is an unknown function of the file /manage_payment.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-12608	A security flaw has been discovered in itsourcecode Online Loan Management System 1.0. The affected element is an unknown function of the file /manage_user.php. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-64104	LangGraph SQLite Checkpoint is an implementation of LangGraph CheckpointSaver that uses SQLite DB (both sync and async, via aiosqlite). Prior to 2.0.11, LangGraph's SQLite store implementation contains SQL injection vulnerabilities using direct string concatenation without proper parameterization, allowing attackers to inject arbitrary SQL and bypass access controls. This vulnerability is fixed in 2.0.11.	7.3	More Details
CVE-2025-43941	Dell Unity, version(s) 5.5 and Prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary command with root privileges. This vulnerability only affects systems without a valid license install.	7.2	More Details
CVE-2025-36137	IBM Sterling Connect Direct for Unix 6.2.0.7 through 6.2.0.9 iFix004, 6.4.0.0 through 6.4.0.2 iFix001, and 6.3.0.2 through 6.3.0.5 iFix002 incorrectly assigns permissions for maintenance tasks to Control Center Director (CCD) users that could allow a privileged user to escalate their privileges further due to unnecessary privilege assignment for post update scripts.	7.2	More Details
CVE-2025-11995	The Community Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via event details parameter in all versions up to, and including, 1.5.2 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-2025-62369	Xibo is an open source digital signage platform with a web content management system (CMS). Versions 4.3.0 and below contain a Remote Code Execution vulnerability in the CMS Developer menu's Module Templating functionality, allowing authenticated users with "System -> Add/Edit custom modules and templates" permissions to manipulate Twig filters and execute arbitrary server-side functions as the web server user. This issue is fixed in version 4.3.1. To workaround this issue, use the 4.1 and 4.2 patch commits.	7.2	More Details
CVE-2025-11733	The Footnotes Made Easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 3.0.7 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-2025-54763	FutureNet MA and IP-K series provided by Century Systems Co., Ltd. contain an OS command Injection vulnerability. A user who logs in to the Web UI of the product may execute an arbitrary OS command.	7.2	More Details
CVE-2025-64168	Agno is a multi-agent framework, runtime and control plane. From 2.0.0 to before 2.2.2, under high concurrency, when session_state is passed to Agent or Team during run or arun calls, a race condition can occur, causing a session_state to be assigned and persisted to the incorrect session. This may result in user data from one session being exposed to another user. This has been patched in version 2.2.2.	7.1	More Details
CVE-2025-43338	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.8.2, iOS 26 and iPadOS 26. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	7.1	More Details
CVE-2025-	JumpServer is an open source bastion host and an operation and maintenance security audit system. Prior to v3.10.21-lts and v4.10.12-lts, a low-privileged authenticated user can invoke LDAP configuration tests and start LDAP synchronization by sending crafted messages to the /ws/ldap/ WebSocket endpoint, bypassing	7.1	More Details

62795	authorization checks and potentially exposing LDAP credentials or causing unintended sync operations. This vulnerability is fixed in v3.10.21-lts and v4.10.12-lts.		
CVE-2025-64348	ELOG allows an authenticated user to modify or overwrite the configuration file, resulting in denial of service. If the execute facility is specifically enabled with the "-x" command line flag, attackers could execute OS commands on the host machine. By default, ELOG is not configured to allow shell commands or self-registration.	7.1	More Details
CVE-2025-12531	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	7.1	More Details
CVE-2025-57107	Kitware VTK (Visualization Toolkit) through 9.5.0 contains a heap buffer overflow vulnerability in vtkGLTFDocumentLoader. When processing specially crafted GLTF files, the copy constructor of Accessor objects fails to properly validate buffer boundaries before performing memory read operations.	7.1	More Details
CVE-2025-60075	Cross-Site Request Forgery (CSRF) vulnerability in Allegro Marketing hpb seo plugin for WordPress hpbseo allows Reflected XSS.This issue affects hpb seo plugin for WordPress: from n/a through <= 3.0.1.	7.1	More Details
CVE-2025-43386	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	7.1	More Details
CVE-2025-64134	Jenkins JDepend Plugin 1.3.1 and earlier includes an outdated version of JDepend Maven Plugin that does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.1	More Details
CVE-2025-10280	IdentityIQ 8.5, IdentityIQ 8.4 and all 8.4 patch levels prior to 8.4p4, IdentityIQ 8.3 and all 8.3 patch levels prior to 8.3p6, and all prior versions allows some IdentityIQ web services that provide non-HTML content to be accessed via a URL path that will set the Content-Type to HTML allowing a requesting browser to interpret content not properly escaped to prevent Cross-Site Scripting (XSS).	7.1	More Details
CVE-2025-48397	The privileged user could log in without sufficient credentials after enabling an application protocol. This security issue has been fixed in the latest script patch latest version of of Eaton BLSS (7.3.0.SCP004).	7.1	More Details
CVE-2025-63675	cryptidy through 1.2.4 allows code execution via untrusted data because pickle.loads is used. This occurs in aes_decrypt_message in symmetric_encryption.py.	6.9	More Details
CVE-2025-60892	An issue in Raspberry Pi Imager version 1.9.6 for Windows, affecting its OS customization feature. The imager's 'public-key authentication' setting unintentionally re-adds a user's id_rsa.pub key from their local Windows machine to the authorized_keys file on the Raspberry Pi, even after the user explicitly deletes the key from the user interface. This creates an unintended attack surface, as it could allow an attacker to use a different key than the intended one to login to the device.	6.8	More Details
CVE-2025-8385	The Zombify plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.7.5. This is due to insufficient input validation in the zf_get_file_by_url function. This makes it possible for authenticated attackers, with subscriber-level access and above, to read arbitrary files on the server, including sensitive system files like /etc/passwd, via a forged request. It's worth noting that successfully exploiting this vulnerability relies on a race condition as the file generated will be deleted immediately.	6.8	More Details
CVE-2025-20741	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00434422; Issue ID: MSV-3958.	6.7	More Details
CVE-2025-20749	In charger, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09915493; Issue ID: MSV-3800.	6.7	More Details
CVE-2025-20748	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00432679; Issue ID: MSV-3950.	6.7	More Details
CVE-2025-20747	In gnss service, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10010443; Issue ID: MSV-3966.	6.7	More Details
CVE-2025-20746	In gnss service, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10010441; Issue ID: MSV-3967.	6.7	More Details
	memoQ 10.1.13.ef1b2b52aae and earlier contains an unquoted service path vulnerability in the memoQ Auto		

CVE-2025-60320	Update Service (memoQauhlp101). The affected service is installed with a path containing spaces and without surrounding quotes. This misconfiguration allows local users to escalate privileges to SYSTEM by placing a malicious executable at C:\Program.exe.	6.7	More Details
CVE-2025-11906	A vulnerability exists in Progress Flowmon versions prior 12.5.6 where certain system configuration files have incorrect file permissions, allowing a user with access to the default flowmon system user account used for SSH access to potentially escalate privileges to root during service initialization.	6.7	More Details
CVE-2025-20739	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00435340; Issue ID: MSV-4038.	6.7	More Details
CVE-2025-20738	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00435342; Issue ID: MSV-4039.	6.7	More Details
CVE-2025-20736	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00435347; Issue ID: MSV-4049.	6.7	More Details
CVE-2025-20730	In preloader, there is a possible escalation of privilege due to an insecure default value. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10068463; Issue ID: MSV-4141.	6.7	More Details
CVE-2025-46556	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Versions 2.27.1 and below allow attackers to permanently corrupt issue activity logs by submitting extremely long notes (tested with 4,788,761 characters) due to a lack of server-side validation of note length. Once such a note is added, the activity stream UI fails to render; therefore, new notes cannot be displayed, effectively breaking all future collaboration on the issue. This issue is fixed in version 2.27.2.	6.5	More Details
CVE-2025-43507	A privacy issue was addressed by moving sensitive data. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, visionOS 26.1. An app may be able to fingerprint the user.	6.5	More Details
CVE-2025-64283	Authorization Bypass Through User-Controlled Key vulnerability in Rometheme RTMKit rometheme-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RTMKit: from n/a through <= 1.6.7.	6.5	More Details
CVE-2025-64354	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matias Ventura Gutenberg gutenberg allows Stored XSS.This issue affects Gutenberg: from n/a through <= 21.8.2.	6.5	More Details
CVE-2025-64361	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StylemixThemes Consulting Elementor Widgets consulting-elementor-widgets allows DOM-Based XSS.This issue affects Consulting Elementor Widgets: from n/a through <= 1.4.2.	6.5	More Details
CVE-2025-35021	By failing to authenticate three times to an unconfigured Abilis CPX device via SSH, an attacker can login to a restricted shell on the fourth attempt, and from there, relay connections.	6.5	More Details
CVE-2025-29699	NetSurf 3.11 is vulnerable to Use After Free in dom_node_set_text_content function.	6.5	More Details
CVE-2025-45663	An issue in NetSurf v3.11 causes the application to read uninitialized heap memory when creating a dom_event structure.	6.5	More Details
CVE-2024-51317	An issue in NetSurf v.3.11 allows a remote attacker to execute arbitrary code via the dom_node_normalize function	6.5	More Details
CVE-2025-63294	WorkDo HRM SaaS HR and Payroll Tool 8.1 is affected vulnerable to Insecure Permissions. An authenticated user can create leave or resignation records on behalf of other users.	6.5	More Details
CVE-2025-43448	This issue was addressed with improved validation of symlinks. This issue is fixed in visionOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. An app may be able to break out of its sandbox.	6.5	More Details
CVE-2025-	A file quarantine bypass was addressed with additional checks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to break out of its sandbox.	6.5	More Details

43412			
CVE-2025-64220	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ReyCommerce Rey Core rey-core allows Stored XSS.This issue affects Rey Core: from n/a through <= 3.1.8.	6.5	More Details
CVE-2025-47370	Transient DOS when a remote device sends an invalid connection request during BT connectable LE scan.	6.5	More Details
CVE-2025-64197	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sizam Rehub rehub-theme allows Stored XSS.This issue affects Rehub: from n/a through < 19.9.9.1.	6.5	More Details
CVE-2025-43457	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. Processing maliciously crafted web content may lead to an unexpected Safari crash.	6.5	More Details
CVE-2025-64365	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in colabrio Ohio Extra ohio-extra allows DOM-Based XSS.This issue affects Ohio Extra: from n/a through <= 3.6.0.	6.5	More Details
CVE-2025-12503	EasyFlow .NET and EasyFlow AiNet developed by Digiwin has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2025-63293	FairSketch Rise Ultimate Project Manager & CRM 3.9.4 is vulnerable to Insecure Permissions. A remote authenticated user can append comments or upload attachments to tickets for which they lack view or edit authorization, due to missing authorization checks in the ticketing/commenting API.	6.5	More Details
CVE-2025-64367	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Adrian Tobey Groundhogg groundhogg allows Stored XSS.This issue affects Groundhogg: from n/a through <= 4.2.6.	6.5	More Details
CVE-2025-60542	SQL Injection vulnerability in TypeORM before 0.3.26 via crafted request to repository.save or repository.update due to the sqlstring call using stringifyObjects default to false.	6.5	More Details
CVE-2025-11758	The All in One Time Clock Lite plugin for WordPress is vulnerable to unauthorized access due to a missing authorization check in all versions up to, and including, 2.0.3. This is due to the plugin exposing admin-level AJAX actions to unauthenticated users via wp_ajax_nopriv_ hooks, while relying only on a nonce check without capability checks. This makes it possible for unauthenticated attackers to create published pages, create shift records with integrity issues, and download time reports containing PII (employee names and work schedules).	6.5	More Details
CVE-2025-64202	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TieLabs Sahifa sahifa allows DOM-Based XSS.This issue affects Sahifa: from n/a through < 5.8.6.	6.5	More Details
CVE-2025-64204	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeSphere SmartMag smart-mag allows Stored XSS.This issue affects SmartMag: from n/a through <= 10.3.1.	6.5	More Details
CVE-2025-64208	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TieLabs Jannah - Extensions jannah-extensions allows DOM-Based XSS.This issue affects Jannah - Extensions: from n/a through <= 1.1.4.	6.5	More Details
CVE-2025-64362	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SeventhQueen K Elements k-elements allows DOM-Based XSS.This issue affects K Elements: from n/a through < 5.5.0.	6.5	More Details
CVE-2025-36092	IBM Cloud Pak For Business Automation 25.0.0, 24.0.1, and 24.0.0 could allow an authenticated user to cause a denial of service due to the improper validation of input length.	6.5	More Details
CVE-2025-64194	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress Eduma eduma allows Stored XSS.This issue affects Eduma: from n/a through <= 5.7.6.	6.5	More Details
CVE-2025-10875	Improper Neutralization of Input Used for LLM Prompting vulnerability in Salesforce Mulesoft Anypoint Code Builder allows Code Injection.This issue affects Mulesoft Anypoint Code Builder: before 1.11.6.	6.5	More Details

CVE-2025-54327	An issue was discovered in VTS in Samsung Mobile Processor and Wearable Processor Exynos 1280, 2200, 1380, W920, W930, W1000. Improper input validation in the VTS driver leads to an arbitrary write.	6.5	More Details
CVE-2025-9544	The Doppler Forms WordPress plugin through 2.5.1 registers an AJAX action install_extension without verifying user capabilities or using a nonce. As a result, any authenticated user — including those with the Subscriber role — can install and activate additional Doppler Forms WordPress plugin through 2.5.1 (limited to those whitelisted by the main Doppler Forms WordPress plugin through 2.5.1).	6.5	More Details
CVE-2025-60319	PerfreeBlog v4.0.11 is vulnerable to Server-Side Request Forgery due to a missing authorization check in the uploadAttachByUrl API endpoint (AttachController.java).	6.5	More Details
CVE-2025-43440	This issue was addressed with improved checks This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	6.5	More Details
CVE-2025-10930	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Currency allows Cross Site Request Forgery.This issue affects Currency: from 0.0.0 before 3.5.0.	6.5	More Details
CVE-2025-11627	The Site Checkup Debug AI Troubleshooting with Wizard and Tips for Each Issue plugin for WordPress is vulnerable to log file poisoning in all versions up to, and including, 1.47. This makes it possible for unauthenticated attackers to insert arbitrary content into log files, and potentially cause denial of service via disk space exhaustion.	6.5	More Details
CVE-2025-63563	Summer Pearl Group Vacation Rental Management Platform prior to v1.0.2 does not properly invalidate active user sessions after a password change. This allows an attacker with a valid session token to maintain access to the account even after the legitimate user changes their password.	6.5	More Details
CVE-2025-63608	A SQL injection vulnerability exists in CSZ-CMS <=1.3.0 in the Form Builder view functionality. The vulnerability is located in the field parameter of the form viewing feature, allowing authenticated administrators to execute arbitrary SQL queries.	6.5	More Details
CVE-2025-64318	Improper Neutralization of Input Used for LLM Prompting vulnerability in Salesforce Mulesoft Anypoint Code Builder allows Manipulating Writeable Configuration Files.This issue affects Mulesoft Anypoint Code Builder: before 1.11.6.	6.5	More Details
CVE-2025-11705	The Anti-Malware Security and Brute-Force Firewall plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 4.23.81 due to a missing capability check combined with an information exposure in several GOTMLS_* AJAX actions. 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-2025-57109	Kitware VTK (Visualization Toolkit) 9.5.0 is vulnerable to Heap Use-After-Free in vtkGLTFImporter::ImportActors. When processing GLTF files with invalid scene node references, the application accesses string members of mesh objects that have been previously freed during actor import operations.	6.5	More Details
CVE-2025-64320	Improper Neutralization of Input Used for LLM Prompting vulnerability in Salesforce Agentforce Vibes Extension allows Code Injection.This issue affects Agentforce Vibes Extension: before 3.2.0.	6.5	More Details
CVE-2025-11740	The wpForo Forum plugin for WordPress is vulnerable to SQL Injection via the Subscriptions Manager in all versions up to, and including, 2.4.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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-2025-54335	An issue was discovered in the GPU driver in Samsung Mobile Processor Exynos 1480, 2400, 1580, 2500. There is a use-after-free in the Xclipse GPU Driver.	6.5	More Details
CVE-2025-52910	An issue was discovered in the GPU in Samsung Mobile Processor and Wearable Processor Exynos 1280, 2200, 1330, 1380, 1480, 2400. A Use-After-Free leads to privilege escalation.	6.5	More Details
CVE-2025-54471	NeuVector used a hard-coded cryptographic key embedded in the source code. At compilation time, the key value was replaced with the secret key value and used to encrypt sensitive configurations when NeuVector stores the data.	6.5	More Details
CVE-	The Schema Scalpel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping when outputting		More

2025-12118	user-supplied data into JSON-LD schema markup. 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	Details
CVE-2025-36172	IBM Cloud Pak for Business Automation 25.0.0 through 25.0.0 Interim Fix 001, 24.0.1 through 24.0.1 Interim Fix 004, 24.0.0 through 24.0.0 Interim Fix 006, and earlier unsupported releases IBM Business Automation Workflow is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2025-11812	The Reuse Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'reuse_builder_single_post_title' shortcode in all versions up to, and including, 1.7. This is due to insufficient input sanitization and output escaping on the 'style' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-6988	The kallyas theme for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's shortcodes in all versions up to, and including, 4.23.0 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-2025-12369	The Extensions for Leaflet Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `geojsonmarker` shortcode in all versions up to, and including, 4.7. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12090	The Employee Spotlight – Team Member Showcase & Meet the Team Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Social URLs in all versions up to, and including, 5.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11502	The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'saswp_tiny_multiple_faq' shortcode in all versions up to, and including, 1.51 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-2025-12324	The TablePress – Tables in WordPress made easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `table` shortcode attributes in all versions up to, and including, 3.2.3 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-2025-11922	The Inactive Logout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ina_redirect_page_individual_user' parameter in all versions up to, and including, 3.5.5 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.	6.4	More Details
CVE-2025-12045	The Orbit Fox: Duplicate Page, Menu Icons, SVG Support, Cookie Notice, Custom Fonts & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the category and tag 'name' parameters in all versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12475	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'blocksy_newsletter_subscribe' shortcode in all versions up to, and including, 2.1.14 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-2025-11806	The Qzzr Shortcode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'qzzr' shortcode in all versions up to, and including, 1.0.1. This is due to insufficient input sanitization and output escaping on the 'quiz' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11841	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Chart Data attributes in all versions up to, and including, 12.2.7 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	6.4	More Details

	injected page.		
CVE-2025-12612	A security flaw has been discovered in Campcodes School Fees Payment Management System 1.0. This issue affects some unknown processing of the file /ajax.php. The manipulation results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-5347	Zohocorp ManageEngine Exchange Reporter Plus versions before 5723 are vulnerable to Stored Cross Site Scripting in the reports module.	6.3	More Details
CVE-2025-5343	Zohocorp ManageEngine Exchange Reporter Plus versions through 5721 are vulnerable to Stored Cross Site Scripting in the Instant Search option.	6.3	More Details
CVE-2025-54384	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.9 and 2.11.4, the helpers.markdown_extract() function did not perform sufficient sanitization of input data before wrapping in an HTML literal element. This helper is used to render user-provided data on dataset, resource, organization or group pages (plus any page provided by an extension that used that helper function), leading to a potential XSS vector. This vulnerability has been fixed in CKAN 2.10.9 and 2.11.4.	6.3	More Details
CVE-2025-63562	Summer Pearl Group Vacation Rental Management Platform prior to v1.0.2 suffers from insufficient server-side authorization. Authenticated attackers can call several endpoints and perform create/update/delete actions on resources owned by arbitrary users by manipulating request parameters (e.g., owner or resource id).	6.3	More Details
CVE-2025-10928	Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Access code allows Brute Force.This issue affects Access code: from 0.0.0 before 2.0.5.	6.3	More Details
CVE-2025-60711	Protection mechanism failure in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	6.3	More Details
CVE-2025-43414	A permissions issue was addressed with improved validation. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. A shortcut may be able to access files that are normally inaccessible to the Shortcuts app.	6.2	More Details
CVE-2025-33176	NVIDIA RunAI for all platforms contains a vulnerability where a user could cause an improper restriction of communications channels on an adjacent network. A successful exploit of this vulnerability might lead to escalation of privileges, data tampering, and information disclosure.	6.2	More Details
CVE-2025-12464	A stack-based buffer overflow was found in the QEMU e1000 network device. The code for padding short frames was dropped from individual network devices and moved to the net core code. The issue stems from the device's receive code still being able to process a short frame in loopback mode. This could lead to a buffer overrun in the e1000_receive_iov() function via the loopback code path. A malicious guest user could use this vulnerability to crash the QEMU process on the host, resulting in a denial of service.	6.2	More Details
CVE-2025-61431	A reflected cross-site scripted (XSS) vulnerability in the /jsp/gsfr_feditorHTML.jsp endpoint of Zucchetti ZMaintenance Infinity and Infinity Zucchetti v4.1 and earlier allows attackers to execute arbitrary Javascript in the context of a user's browser via injecting a crafted payload into the pHtmlSource parameter. A vendor fix was released on 2025-06-18.	6.1	More Details
CVE-2025-12450	The LiteSpeed Cache plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URLs in all versions up to, and including, 7.5.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-63447	Water Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in /add_customer.php.	6.1	More Details
CVE-2025-50574	Cross-site scripting (XSS) vulnerability in blog-details.php in Hiruna Gallage's Glamour Salon Management System v1 allows remote attackers to inject arbitrary web script or HTML via the blog comment section parameter.	6.1	More Details
CVE-2025-63446	Water Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in /add_vendor.php.	6.1	More Details
CVE-2025-47362	Information disclosure while processing message from client with invalid payload.	6.1	More Details

CVE-2025-50736	An open redirect vulnerability exists in Byaidu PDFMathTranslate v1.9.9 that allows attackers to craft URLs that cause the application to redirect users to arbitrary external websites via the file parameter to the /gradio_api endpoint. This vulnerability could be exploited for phishing attacks or to bypass security filters.	6.1	More Details
CVE-2025-12402	The LinkedIn Resume plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.00. This is due to missing or incorrect nonce validation on the linkedinresume_printAdminPage() 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-2025-27064	Information disclosure while registering commands from clients with diag through diagHal.	6.1	More Details
CVE-2025-12401	The Label Plugins plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.5. This is due to missing or incorrect nonce validation on the label_plugins_options() 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-2025-63448	Water Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in /edit_product.php?id=1.	6.1	More Details
CVE-2025-12400	The LMB^Box Smileys plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2. This is due to missing or incorrect nonce validation on the manage_page() 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-2025-61427	A reflected cross-site scripting (XSS) vulnerability in BEO GmbH BEO Atlas Einfuhr Ausfuhr 3.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload into the userid and password parameters.	6.1	More Details
CVE-2025-12403	The Associados Amazon Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.8. This is due to missing or incorrect nonce validation on the brzon_admin_panel() 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-2025-64100	CKAN is an open-source DMS (data management system) for powering data hubs and data portals. Prior to 2.10.9 and 2.11.4, session ids could be fixed by an attacker if the site is configured with server-side session storage (CKAN uses cookie-based session storage by default). The attacker would need to either set a cookie on the victim's browser or steal the victim's currently valid session. Session identifiers are now regenerated after each login. This vulnerability has been fixed in CKAN 2.10.9 and 2.11.4	6.1	More Details
CVE-2025-10926	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal JSON Field allows Cross-Site Scripting (XSS).This issue affects JSON Field: from 0.0.0 before 1.5.	6.1	More Details
CVE-2025-10927	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Plausible tracking allows Cross-Site Scripting (XSS).This issue affects Plausible tracking: from 0.0.0 before 1.0.2.	6.1	More Details
CVE-2025-52180	Cross-site scripting (XSS) vulnerability in Zucchetti Ad Hoc Infinity 4.2 and earlier allows remote unauthenticated attackers to inject arbitrary JavaScript via the pHtmlSource parameter of the /ahi/jsp/gsfr_feditorHTML.jsp?pHtmlSource endpoint.	6.1	More Details
CVE-2025-52179	Cross-site scripting (XSS) vulnerability in Zucchetti Ad Hoc Revolution 4.1 and earlier allows remote unauthenticated attackers to inject arbitrary JavaScript via the pHtmlSource parameter of the /ahrw/jsp/gsfr_feditorHTML.jsp endpoint.	6.1	More Details
CVE-2025-12410	The SH Contextual Help plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.1. This is due to missing or incorrect nonce validation in the sh_contextual_help_dashboard_widget() function. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-56313	A Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the /publix/run endpoint of JATOS 3.7.1 through 3.9.6 (inclusive). This allows remote attackers to execute arbitrary JavaScript in a user's web browser by including a malicious payload in the "code" URL parameter. When an authenticated admin user accesses the study's URL, the malicious script gets interpreted and executes within their browser, which can lead to unauthorized actions, account compromise, and privilege escalation.	6.1	More Details
CVE-	A stored cross-site scripting (XSS) vulnerability in AIxBlock commit 04f305 allows attackers to execute		More

2025-63885	arbitrary web scripts or HTML via injecting a crafted payload into the model_desc field.	6.1	Details
CVE-2025-12083	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal CivicTheme Design System allows Cross-Site Scripting (XSS).This issue affects CivicTheme Design System: from 0.0.0 before 1.12.0.	6.1	More Details
CVE-2025-60950	An arbitrary file upload vulnerability in the Data Preparation function of AIxBlock commit f60975 allows attackers to execute arbitrary code via a crafted SVG file.	6.1	More Details
CVE-2025-12456	The Centangle-Team plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to modify plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Additionally, due to insufficient input sanitization and output escaping on cai_name_color parameter, this issue allows to inject arbitrary web scripts in pages, that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2025-12142	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in ABB Terra AC wallbox.This issue affects Terra AC wallbox: through 1.8.33.	6.1	More Details
CVE-2025-12452	The Visit Counter plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the widgets.php 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-2025-12412	The Top Bar Notification plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12. This is due to missing or incorrect nonce validation on th tbn_ajax_add() function. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-12415	The MapMap plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the admin_shortcode_submit, admin_configuration_submit, and admin_shortcode_delete functions. This makes it possible for unauthenticated attackers to update the plugin's 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-2025-12416	The Pagerank Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Cross-Site Request Forgery in all versions up to, and including, 1.1.5. This is due to missing nonce validation on the pr_save_settings() function and insufficient input sanitization. This makes it possible for unauthenticated attackers to inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The injected scripts will execute whenever a user accesses the plugin's settings page.	6.1	More Details
CVE-2025-64135	Jenkins Eggplant Runner Plugin 0.0.1.301.v963cffe8ddb_8 and earlier sets the Java system property `jdk.http.auth.tunneling.disabledSchemes` to an empty value, disabling a protection mechanism of the Java runtime.	5.9	More Details
CVE-2025-49042	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WooCommerce woocommerce allows Stored XSS.This issue affects WooCommerce: from n/a through 10.0.2.	5.9	More Details
CVE-2025-12695	The overly permissive sandbox configuration in DSPy allows attackers to steal sensitive files in cases when users build an AI agent which consumes user input and uses the “PythonInterpreter” class.	5.9	More Details
CVE-2025-54549	Cryptographic validation of upgrade images could be circumventing by dropping a specifically crafted file into the upgrade ISO	5.9	More Details
CVE-2025-64291	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Premmerce Premmerce User Roles premmerce-user-roles allows Stored XSS.This issue affects Premmerce User Roles: from n/a through <= 1.0.13.	5.9	More Details
CVE-2025-64289	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Premmerce Premmerce Product Search for WooCommerce premmerce-search allows Stored XSS.This issue affects Premmerce Product Search for WooCommerce: from n/a through <= 2.2.4.	5.9	More Details
CVE-2025-64200	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Email Template Customizer for WooCommerce email-template-customizer-for-woo allows Stored XSS.This issue affects Email Template Customizer for WooCommerce: from n/a through <= 1.2.17.	5.9	More Details

CVE-2025-60898	An unauthenticated server-side request forgery (SSRF) vulnerability in the Thumbnail via-uri endpoint of Halo CMS 2.21 allows a remote attacker to cause the server to issue HTTP requests to attacker-controlled URLs, including internal addresses. The endpoint performs a server-side GET to a user-supplied URI without adequate allow/blocklist validation and returns a 307 redirect that can disclose internal URLs in the Location header.	5.8	More Details
CVE-2025-43391	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in iOS 26.1 and iPadOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43447	The issue was addressed with improved memory handling. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, visionOS 26.1. An app may be able to cause unexpected system termination or corrupt kernel memory.	5.5	More Details
CVE-2025-43335	The issue was addressed by adding additional logic. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2025-43345	A correctness issue was addressed with improved checks. This issue is fixed in tvOS 26, watchOS 26, macOS Sonoma 14.8, iOS 26 and iPadOS 26, macOS Sequoia 15.7, visionOS 26, iOS 18.7 and iPadOS 18.7. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43348	A logic issue was addressed with improved validation. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may bypass Gatekeeper checks.	5.5	More Details
CVE-2025-43398	The issue was addressed with improved memory handling. This issue is fixed in visionOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2025-43396	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. A sandboxed app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43499	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43322	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2025-43390	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.7.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2025-43394	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access protected user data.	5.5	More Details
CVE-2025-43397	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2025-43382	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43288	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Sequoia 15.7. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2025-43378	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43446	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2025-	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	5.5	More Details

43477			
CVE-2025-43377	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.2. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2025-43478	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2025-43479	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43360	The issue was addressed with improved UI. This issue is fixed in iOS 26 and iPadOS 26. Password fields may be unintentionally revealed.	5.5	More Details
CVE-2025-43426	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 26.1 and iPadOS 26.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43379	This issue was addressed with improved validation of symlinks. This issue is fixed in visionOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. An app may be able to access protected user data.	5.5	More Details
CVE-2025-43498	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.1 and iPadOS 26.1, macOS Sequoia 15.7.2, macOS Sonoma 14.8.2, visionOS 26.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43455	A privacy issue was addressed with improved checks. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, visionOS 26.1. A malicious app may be able to take a screenshot of sensitive information in embedded views.	5.5	More Details
CVE-2025-43411	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2025-43380	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. Parsing a file may lead to an unexpected app termination.	5.5	More Details
CVE-2025-11193	A potential vulnerability was reported in some Lenovo Tablets that could allow a local authenticated user or application to gain access to sensitive device specific information.	5.5	More Details
CVE-2025-43334	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2025-43495	The issue was addressed with improved checks. This issue is fixed in iOS 26.1 and iPadOS 26.1. An app may be able to monitor keystrokes without user permission.	5.4	More Details
CVE-2025-64368	Cross-Site Request Forgery (CSRF) vulnerability in Mikado-Themes Bard bardwp allows Cross Site Request Forgery.This issue affects Bard: from n/a through <= 1.6.	5.4	More Details
CVE-2025-63443	School Management System PHP v1.0 is vulnerable to Cross Site Scripting (XSS) in /login.php via the password parameter.	5.4	More Details
CVE-2025-64132	Jenkins MCP Server Plugin 0.84.v50ca_24ef83f2 and earlier does not perform permission checks in multiple MCP tools, allowing attackers to trigger builds and obtain information about job and cloud configuration they should not be able to access.	5.4	More Details
CVE-2025-64133	A cross-site request forgery (CSRF) vulnerability in Jenkins Extensible Choice Parameter Plugin 239.v5f5c278708cf and earlier allows attackers to execute sandboxed Groovy code.	5.4	More Details
CVE-2025-30191	Malicious content from E-Mail can be used to perform a redressing attack. Users can be tricked to perform unintended actions or provide sensitive information to a third party which would enable further threats. Attribute values containing HTML fragments are now denied by the sanitization procedure. No publicly available exploits are known	5.4	More Details

CVE-2025-63449	Water Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in /orders.php.	5.4	More Details
CVE-2025-64150	A missing permission check in Jenkins Publish to Bitbucket Plugin 0.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	5.4	More Details
CVE-2025-64149	A cross-site request forgery (CSRF) vulnerability in Jenkins Publish to Bitbucket Plugin 0.4 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	5.4	More Details
CVE-2025-64212	Missing Authorization vulnerability in StylemixThemes MasterStudy LMS Pro masterstudy-lms-learning-management-system-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MasterStudy LMS Pro: from n/a through < 4.7.16.	5.4	More Details
CVE-2025-50363	Phpgurukul Maid Hiring Management System 1.0 is vulnerable to Cross Site Scripting (XSS) in /maid-hiring.php va the name field.	5.4	More Details
CVE-2025-64285	Missing Authorization vulnerability in Premmerce Premmerce Wholesale Pricing for WooCommerce premmerce-woocommerce-wholesale-pricing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Premmerce Wholesale Pricing for WooCommerce: from n/a through <= 1.1.10.	5.4	More Details
CVE-2025-12413	The Social Media WPCF7 Stop Words plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.3. This is due to missing or incorrect nonce validation on the smWpCfSwOptions() function. This makes it possible for unauthenticated attackers to update the plugin's 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.	5.4	More Details
CVE-2025-63450	Car-Booking-System-PHP v.1.0 is vulnerable to Cross Site Scripting (XSS) in /carlux/booking.php.	5.4	More Details
CVE-2025-64210	Missing Authorization vulnerability in StylemixThemes Masterstudy Elementor Widgets masterstudy-elementor-widgets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Masterstudy Elementor Widgets: from n/a through <= 1.2.4.	5.4	More Details
CVE-2025-55155	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions 2.27.1 and below, when a user edits their profile to change their e-mail address, the system saves it without validating that it actually belongs to the user. This could result in storing an invalid email address, preventing the user from receiving system notifications. Notifications sent to another person's email address could lead to information disclosure. This issue is fixed in version 2.27.2.	5.4	More Details
CVE-2025-36592	Dell Secure Connect Gateway (SCG) Policy Manager, version(s) 5.20. 5.22, 5.24, 5.26, 5.28, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Script injection.	5.4	More Details
CVE-2025-62402	API users via `/api/v2/dagReports` could perform Dag code execution in the context of the api-server if the api-server was deployed in the environment where Dag files were available.	5.4	More Details
CVE-2025-20731	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege (when OceReducedNeighborReport is disabled). User interaction is not needed for exploitation. Patch ID: WCNCR00441511; Issue ID: MSV-4140.	5.3	More Details
CVE-2025-20732	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege (when OceReducedNeighborReport is disabled). User interaction is not needed for exploitation. Patch ID: WCNCR00441510; Issue ID: MSV-4139.	5.3	More Details
CVE-2025-20734	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00441507; Issue ID: MSV-4112.	5.3	More Details
CVE-2025-64199	Missing Authorization vulnerability in WpEstate wpresidence wpresidence allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects wpresidence: from n/a through <= 5.3.2.	5.3	More Details
CVE-	The issue was addressed with improved handling of caches. This issue is fixed in Safari 26.1, visionOS 26.1,		More

2025-43392	watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. A website may exfiltrate image data cross-origin.	5.3	Details
CVE-2025-64296	Missing Authorization vulnerability in Facebook Facebook for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Facebook for WooCommerce: from n/a through 3.5.7.	5.3	More Details
CVE-2025-54330	An issue was discovered in NPU in Samsung Mobile Processor Exynos through July 2025. There is an Out-of-bounds Read of q->bufs[] in the __is_done_for_me function.	5.3	More Details
CVE-2025-43444	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1. An app may be able to fingerprint the user.	5.3	More Details
CVE-2025-54331	An issue was discovered in NPU in Samsung Mobile Processor Exynos through July 2025. There is an Untrusted Pointer Dereference of src_hdr in the copy_ncp_header function.	5.3	More Details
CVE-2025-60925	codeshare v1.0.0 was discovered to contain an information leakage vulnerability.	5.3	More Details
CVE-2025-54325	An issue was discovered in VTS in Samsung Mobile Processor and Wearable Processor Exynos 1080, 1280, 2200, 1380, 1480, 2400, 1580, 2500, W920, W930, W1000. A race condition in the VTS driver results in an out-of-bounds read, leading to an information leak.	5.3	More Details
CVE-2025-10008	The Translate WordPress and go Multilingual – Weglot plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'clean_options' function in all versions up to, and including, 5.1. This makes it possible for unauthenticated attackers to delete limited transients that contain cached plugin options.	5.3	More Details
CVE-2025-54333	An issue was discovered in NPU in Samsung Mobile Processor Exynos through July 2025. There is an Invalid Pointer Dereference of node in the get_vs4l_profiler_node function.	5.3	More Details
CVE-2025-11816	The Privacy Policy Generator, Terms & Conditions Generator WordPress Plugin : WP Legal Pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the disconnect_account_request() function in all versions up to, and including, 3.5.1. This makes it possible for unauthenticated attackers to disconnect the site from its API plan.	5.3	More Details
CVE-2025-58189	When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.	5.3	More Details
CVE-2025-27374	An issue was discovered in the Secure Boot component in Samsung Mobile Processor and Wearable Processor Exynos 9820, 9825, 980, 990, 850, 1080, 1280, 2200, 1330, 1380, 1480, 2400. The lack of a length check leads to out-of-bounds writes.	5.3	More Details
CVE-2025-11881	The AppPresser – Mobile App Framework plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'myappp_verify' function in all versions up to, and including, 4.5.0. This makes it possible for unauthenticated attackers to extract sensitive data including plugin and theme names and version numbers, which can be used to facilitate targeted attacks against outdated or vulnerable components.	5.3	More Details
CVE-2025-61724	The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU consumption.	5.3	More Details
CVE-2023-7320	The WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 7.8.2, due to improper CORS handling on the Store API's REST endpoints allowing direct external access from any origin. This can allow unauthenticated attackers to extract sensitive user information including PII(Personal Identifiable Information).	5.3	More Details
CVE-2025-64319	Incorrect Permission Assignment for Critical Resource vulnerability in Salesforce Mulesoft Anypoint Code Builder allows Manipulating Writeable Configuration Files.This issue affects Mulesoft Anypoint Code Builder: before 1.11.6.	5.3	More Details
CVE-2025-64321	Improper Neutralization of Input Used for LLM Prompting vulnerability in Salesforce Agentforce Vibes Extension allows Manipulating Writeable Configuration Files.This issue affects Agentforce Vibes Extension: before 3.2.0.	5.3	More Details
CVE-	Incorrect Permission Assignment for Critical Resource vulnerability in Salesforce Agentforce Vibes Extension		More

2025-64322	allows Manipulating Writeable Configuration Files.This issue affects Agentforce Vibes Extension: before 3.2.0.	5.3	Details
CVE-2025-10929	Improper Validation of Consistency within Input vulnerability in Drupal Reverse Proxy Header allows Manipulating User-Controlled Variables.This issue affects Reverse Proxy Header: from 0.0.0 before 1.1.2.	5.3	More Details
CVE-2025-11174	The Document Library Lite plugin for WordPress is vulnerable to Improper Authorization in all versions up to, and including, 1.1.6. This is due to the plugin exposing an unauthenticated AJAX action dll_load_posts which returns a JSON table of document data without performing nonce or capability checks. The handler accepts an attacker-controlled args array where the status option explicitly allows draft, pending, future, and any. This makes it possible for unauthenticated attackers to retrieve unpublished document titles and content via the AJAX endpoint.	5.3	More Details
CVE-2025-58711	Missing Authorization vulnerability in solwin Blog Designer PRO blog-designer-pro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Blog Designer PRO: from n/a through <= 3.4.8.	5.3	More Details
CVE-2025-57931	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Popup box allows Cross Site Request Forgery.This issue affects Popup box: from n/a through 5.5.4.	5.3	More Details
CVE-2025-61959	Prior to September 19, 2025, the Hospital Manager Backend Services returned verbose ASP.NET error pages for invalid WebResource.axd requests, disclosing framework and ASP.NET version information, stack traces, internal paths, and the insecure configuration 'customErrors mode="Off"', which could have facilitated reconnaissance by unauthenticated attackers.	5.3	More Details
CVE-2025-58185	Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.	5.3	More Details
CVE-2025-47912	The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.	5.3	More Details
CVE-2025-58152	FutureNet MA and IP-K series provided by Century Systems Co., Ltd. put the firmware version and the garbage collection information on the internal web page. With some crafted HTTP request, they can be accessed without authentication.	5.3	More Details
CVE-2025-11191	The RealPress WordPress plugin before 1.1.0 registers the REST routes without proper permission checks, allowing the creation of pages and sending of emails from the site.	5.3	More Details
CVE-2025-12094	The OOPSpam Anti-Spam: Spam Protection for WordPress Forms & Comments (No CAPTCHA) plugin for WordPress is vulnerable to IP Header Spoofing in all versions up to, and including, 1.2.53. This is due to the plugin trusting client-controlled forwarded headers (such as CF-Connecting-IP, X-Forwarded-For, and others) without verifying that those headers originate from legitimate, trusted proxies. This makes it possible for unauthenticated attackers to spoof their IP address and bypass IP-based security controls, including blocked IP lists and rate limiting protections, by sending arbitrary HTTP headers with their requests.	5.3	More Details
CVE-2025-64294	Missing Authorization vulnerability in d3wp WP Snow Effect allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Snow Effect: from n/a through 1.1.15.	5.3	More Details
CVE-2025-54547	On affected platforms, if SSH session multiplexing was configured on the client side, SSH sessions (e.g, scp, sftp) multiplexed onto the same channel could perform file-system operations after a configured session timeout expired	5.3	More Details
CVE-2025-64211	Missing Authorization vulnerability in StylemixThemes Masterstudy Elementor Widgets masterstudy-elementor-widgets allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Masterstudy Elementor Widgets: from n/a through <= 1.2.4.	5.3	More Details
CVE-2025-43481	This issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.2. An app may be able to break out of its sandbox.	5.3	More Details
CVE-2025-58186	Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.	5.3	More Details
CVE-2025-	The ERI File Library plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'erifl_file' AJAX action in all versions up to, and including, 1.1.0. This makes it possible	5.3	More

12041	for unauthenticated attackers to download files restricted to specific user roles.		Details
CVE-2025-12157	The Simple User Capabilities plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_nopriv_reset_capability' AJAX endpoint in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to reset any user's capabilities.	5.3	More Details
CVE-2025-12350	The DominoKit plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wp_ajax_nopriv_dominokit_option_admin_action AJAX endpoint in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to update plugin settings.	5.3	More Details
CVE-2025-12521	The Analytify Pro plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.0.3 via the Analytify Tag HTML details. This makes it possible for unauthenticated attackers to extract usernames from source code. While we generally do not assign CVE IDs to username exposure issues, this vendor has specifically requested we consider it a vulnerability.	5.3	More Details
CVE-2025-61876	Insecure Direct Object Reference (IDOR) in /tenants/{id} API endpoint in Inforcer Platform version 2.0.153 allows an authenticated user with low privileges to enumerate and access tenant information belonging to other clients via modification of the tenant ID in the request URL.	5.0	More Details
CVE-2025-12615	A security vulnerability has been detected in PHPGurukul News Portal 1.0. The affected element is an unknown function of the file /onps/settings.py. Such manipulation of the argument SECRET_KEY leads to use of hard-coded cryptographic key . The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is described as difficult. The exploit has been disclosed publicly and may be used.	5.0	More Details
CVE-2025-12657	The KMIP response parser built into mongo binaries is overly tolerant of certain malformed packets, and may parse them into invalid objects. Later reads of this object can result in read access violations.	5.0	More Details
CVE-2015-10146	The Thumbnail Slider With Lightbox plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.0.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-43504	A buffer overflow was addressed with improved bounds checking. This issue is fixed in Xcode 26.1. A user in a privileged network position may be able to cause a denial-of-service.	4.9	More Details
CVE-2015-10147	The Easy Testimonial Slider and Form plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.0.2 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 Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-12137	The Import WP – Export and Import CSV and XML files to WordPress plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 2.14.16. This is due to the plugin's REST API endpoint accepting arbitrary absolute file paths without proper validation in the 'attach_file()' function when handling 'file_local' actions. This makes it possible for authenticated attackers, with administrator-level access and above, to read arbitrary files on the server's filesystem, including sensitive configuration files and system files via the 'local_url' parameter.	4.9	More Details
CVE-2025-59501	Authentication bypass by spoofing in Microsoft Configuration Manager allows an authorized attacker to perform spoofing over an adjacent network.	4.8	More Details
CVE-2025-36093	IBM Cloud Pak For Business Automation 25.0.0, 24.0.1, and 24.0.0 could allow an attacker to access unauthorized content or perform unauthorized actions using man in the middle techniques due to improper access controls.	4.8	More Details
CVE-2025-12609	A vulnerability was found in CodeAstro Gym Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/update-progress.php. Performing manipulation of the argument id/ini_weight results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-12594	A security flaw has been discovered in code-projects Simple Online Hotel Reservation System 2.0. This affects an unknown function of the file /admin/add_account.php. The manipulation of the argument Name results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	4.7	More Details
CVE-2025-	A vulnerability was identified in code-projects Simple Online Hotel Reservation System 2.0. The impacted element is an unknown function of the file /admin/edit_room.php of the component Photo Handler. The	4.7	More

12593	manipulation leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.		Details
CVE-2025-43420	A race condition was addressed with improved state handling. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access sensitive user data.	4.7	More Details
CVE-2025-20740	In wlan STA driver, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00435337; Issue ID: MSV-4036.	4.7	More Details
CVE-2025-12598	A flaw has been found in SourceCodester Best House Rental Management System 1.0. Affected by this issue is the function save_tenant of the file /admin_class.php. Executing manipulation of the argument firstname can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. Other parameters might be affected as well.	4.7	More Details
CVE-2025-12597	A vulnerability was detected in SourceCodester Best House Rental Management System 1.0. Affected by this vulnerability is the function save_category of the file /admin_class.php. Performing manipulation of the argument Name results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	4.7	More Details
CVE-2025-12614	A weakness has been identified in SourceCodester Best House Rental Management System 1.0. Impacted is the function delete_payment of the file /admin_class.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-12610	A vulnerability was determined in CodeAstro Gym Management System 1.0. This affects an unknown part of the file /admin/view-progress-report.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-62503	User with CREATE and no UPDATE privilege for Pools, Connections, Variables could update existing records via bulk create API with overwrite action.	4.6	More Details
CVE-2025-43459	An authentication issue was addressed with improved state management. This issue is fixed in watchOS 26.1. An attacker with physical access to a locked Apple Watch may be able to view Live Voicemail.	4.6	More Details
CVE-2025-43422	The issue was addressed by adding additional logic. This issue is fixed in iOS 26.1 and iPadOS 26.1. An attacker with physical access to a device may be able to disable Stolen Device Protection.	4.6	More Details
CVE-2025-43460	A logic issue was addressed with improved checks. This issue is fixed in iOS 26.1 and iPadOS 26.1. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2025-54941	An example dag `example_dag_decorator` had non-validated parameter that allowed the UI user to redirect the example to a malicious server and execute code on worker. This however required that the example dags are enabled in production (not default) or the example dag code copied to build your own similar dag. If you used the `example_dag_decorator` please review it and apply the changes implemented in Airflow 3.0.5 accordingly.	4.6	More Details
CVE-2025-63442	Simple User Management System with PHP-MySQL v1.0 is vulnerable to Cross-Site Scripting (XSS) via the Profile Section. The system fails to properly sanitize user input, allowing attackers to inject and execute arbitrary JavaScript when the input is displayed in the browser	4.6	More Details
CVE-2024-45161	A CSRF issue was discovered in the administrative web GUI in Blu-Castle BCUM221E 1.0.0P220507. This can be exploited via a URL, an image load, an XMLHttpRequest, etc. and can result in exposure of data or unintended code execution.	4.6	More Details
CVE-2025-40603	A potential exposure of sensitive information in log files in SonicWall SMA100 Series appliances may allow a remote, authenticated administrator, under certain conditions to view partial users credential data.	4.5	More Details
CVE-2025-11927	The Flying Images: Optimize and Lazy Load Images for Faster Page Speed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.4.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-	The CSS & JavaScript Toolbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 12.0.5 due to insufficient input sanitization and output escaping.		More

2025-11928	This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	Details
CVE-2025-12396	The clubmember plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12393	The Free Quotation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.1.6 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.	4.4	More Details
CVE-2025-12371	The Nari Accountant plugin for WordPress is vulnerable to Stored Cross-Site Scripting via account settings in all versions up to, and including, 1.0.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-11753	The Bootstrap Multi-language Responsive Portfolio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12065	The WP Carticon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'carticon_js_script' parameter in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12184	The MeetingList plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-43336	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app with root privileges may be able to access private information.	4.4	More Details
CVE-2025-64146	Jenkins Curseforge Publisher Plugin 1.0 stores API Keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission, or access to the Jenkins controller file system.	4.3	More Details
CVE-2025-64145	Jenkins ByteGuard Build Actions Plugin 1.0 does not mask API tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-43429	A buffer overflow was addressed with improved bounds checking. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-64142	A missing permission check in Jenkins Nexus Task Runner Plugin 0.9.2 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2025-43425	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2023-32199	A vulnerability has been identified within Rancher Manager, where after removing a custom GlobalRole that gives administrative access or the corresponding binding, the user still retains access to clusters. This only affects custom Global Roles that have a * on * in * rule for resources or have a * on * rule for non-resource URLs	4.3	More Details
CVE-2025-64143	Jenkins OpenShift Pipeline Plugin 1.0.57 and earlier stores authorization tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission, or access to the Jenkins controller file system.	4.3	More Details

CVE-2025-43427	This issue was addressed through improved state management. This issue is fixed in iOS 26.1 and iPadOS 26.1, tvOS 26.1, Safari 26.1, visionOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-64136	A cross-site request forgery (CSRF) vulnerability in Jenkins Themis Plugin 1.4.1 and earlier allows attackers to connect to an attacker-specified HTTP server.	4.3	More Details
CVE-2025-64144	Jenkins ByteGuard Build Actions Plugin 1.0 stores API tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission, or access to the Jenkins controller file system.	4.3	More Details
CVE-2025-43430	This issue was addressed through improved state management. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-43384	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1, macOS Sequoia 15.7.2. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	4.3	More Details
CVE-2025-36091	IBM Cloud Pak For Business Automation 25.0.0, 24.0.1, and 24.0.0 could allow an authenticated user to cause dashboards to become inaccessible to legitimate users due to invalid ownership assignment.	4.3	More Details
CVE-2025-64138	A cross-site request forgery (CSRF) vulnerability in Jenkins Start Windocks Containers Plugin 1.4 and earlier allows attackers to connect to an attacker-specified URL.	4.3	More Details
CVE-2025-12626	A security flaw has been discovered in jeecgboot jeewx-boot up to 641ab52c3e1845fec39996d7794c33fb40dad1dd. This affects the function getImgUrl of the file WxActGoldeneggsPrizesController.java. Performing manipulation of the argument imgurl results in path traversal. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The root cause was initially fixed but can be evaded with additional encoding.	4.3	More Details
CVE-2025-43383	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 26.1 and iPadOS 26.1, tvOS 26.1, visionOS 26.1, macOS Sequoia 15.7.2. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	4.3	More Details
CVE-2025-64148	A missing permission check in Jenkins Publish to Bitbucket Plugin 0.4 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2025-64147	Jenkins Curseforge Publisher Plugin 1.0 does not mask API Keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2025-43421	Multiple issues were addressed by disabling array allocation sinking. This issue is fixed in iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2024-58269	A vulnerability has been identified in Rancher Manager, where sensitive information, including secret data, cluster import URLs, and registration tokens, is exposed to any entity with access to Rancher audit logs.	4.3	More Details
CVE-2025-64137	A missing permission check in Jenkins Themis Plugin 1.4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server.	4.3	More Details
CVE-2025-64290	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce Premmerce Product Search for WooCommerce premmerce-search allows Cross Site Request Forgery.This issue affects Premmerce Product Search for WooCommerce: from n/a through <= 2.2.4.	4.3	More Details
CVE-2025-43432	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-64358	Missing Authorization vulnerability in WebToffee Smart Coupons for WooCommerce wt-smart-coupons-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Smart Coupons for WooCommerce: from n/a through <= 2.2.3.	4.3	More Details
CVE-2025-	Missing Authorization vulnerability in f1logic Insert PHP Code Snippet insert-php-code-snippet allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Insert PHP Code Snippet:	4.3	More

64356	from n/a through <= 1.4.3.		Details
CVE-2025-64351	Insertion of Sensitive Information Into Sent Data vulnerability in Rank Math SEO Rank Math SEO seo-by-rank-math allows Retrieve Embedded Sensitive Data.This issue affects Rank Math SEO: from n/a through <= 1.0.252.1.	4.3	More Details
CVE-2025-64139	A missing permission check in Jenkins Start Windocks Containers Plugin 1.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2025-54548	On affected platforms, restricted users could view sensitive portions of the config database via a debug API (e.g., user password hashes)	4.3	More Details
CVE-2025-43503	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. Visiting a malicious website may lead to user interface spoofing.	4.3	More Details
CVE-2025-8383	The Depicter plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions less than, or equal to, 4.0.4. This is due to missing or incorrect nonce validation on the depicter-document-rules-store function. This makes it possible for unauthenticated attackers to modify document rules 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-2025-58183	tar.Reader does not set a maximum size on the number of sparse region data blocks in GNU tar pax 1.0 sparse files. A maliciously-crafted archive containing a large number of sparse regions can cause a Reader to read an unbounded amount of data from the archive into memory. When reading from a compressed source, a small compressed input can result in large allocations.	4.3	More Details
CVE-2025-12175	The The Events Calendar plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the 'tec_qr_code_modal' AJAX endpoint in all versions up to, and including, 6.15.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view draft event names and generate/view QR codes for them.	4.3	More Details
CVE-2025-11975	The FuseWP – WordPress User Sync to Email List & Marketing Automation (Mailchimp, Constant Contact, ActiveCampaign etc.) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_changes() function in all versions up to, and including, 1.1.23.0. This makes it possible for unauthenticated attackers to add and edit sync rules.	4.3	More Details
CVE-2025-12069	The WP Global Screen Options plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.2. This is due to missing nonce validation on the `updatewpglobalscreenoptions` action handler. This makes it possible for unauthenticated attackers to modify global screen options for all users via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12070	The ViaAds plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.1. This is due to missing nonce validation on the `ViaAds_pluginHandler` function. This makes it possible for unauthenticated attackers to modify the plugin's API key and cookie consent settings via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-64288	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce Premmerce premmerce allows Cross Site Request Forgery.This issue affects Premmerce: from n/a through <= 1.3.19.	4.3	More Details
CVE-2025-64286	Cross-Site Request Forgery (CSRF) vulnerability in WpEstate WP Rentals wprentals allows Cross Site Request Forgery.This issue affects WP Rentals: from n/a through <= 3.13.1.	4.3	More Details
CVE-2025-64234	Missing Authorization vulnerability in Evergreen Content Poster Evergreen Content Poster evergreen-content-poster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Evergreen Content Poster: from n/a through <= 1.4.5.	4.3	More Details
CVE-2025-64229	Missing Authorization vulnerability in BoldGrid Client Invoicing by Sprout Invoices sprout-invoices allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Client Invoicing by Sprout Invoices: from n/a through <= 20.8.7.	4.3	More Details
CVE-2025-64228	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in FantasticPlugins SUMO Affiliates Pro affs allows Retrieve Embedded Sensitive Data.This issue affects SUMO Affiliates Pro: from n/a through <= 11.0.0.	4.3	More Details
CVE-2025-64226	Cross-Site Request Forgery (CSRF) vulnerability in colabrio Stockie Extra stockie-extra allows Cross Site Request Forgery.This issue affects Stockie Extra: from n/a through <= 1.2.11.	4.3	More Details

CVE-2025-64219	Missing Authorization vulnerability in Strategy11 Team Business Directory business-directory-plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Business Directory: from n/a through <= 6.4.18.	4.3	More Details
CVE-2025-43434	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. Processing maliciously crafted web content may lead to an unexpected Safari crash.	4.3	More Details
CVE-2025-12188	The Posts Navigation Links for Sections and Headings – Free by WP Masters plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the 'wpm_navigation_links_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-2025-12389	The Import Export For WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_setting() function in all versions up to, and including, 1.6.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's record setting.	4.3	More Details
CVE-2025-64201	Cross-Site Request Forgery (CSRF) vulnerability in blubrry PowerPress Podcasting powerpress allows Cross Site Request Forgery.This issue affects PowerPress Podcasting: from n/a through <= 11.13.12.	4.3	More Details
CVE-2025-58939	Cross-Site Request Forgery (CSRF) vulnerability in highwarden Super Store Finder superstorefinder-wp allows Cross Site Request Forgery.This issue affects Super Store Finder: from n/a through <= 7.5.	4.3	More Details
CVE-2025-46363	Dell Secure Connect Gateway (SCG) 5.0 Application and Appliance version(s) 5.26.00.00 - 5.30.00.00, contain a Relative Path Traversal vulnerability in the SCG exposed for an internal collection download REST API (if this REST API is enabled by Admin user from UI). A low privileged attacker with remote access could potentially exploit this vulnerability, leading to allowing relative path traversal to restricted resources.	4.3	More Details
CVE-2025-5342	Zohocorp ManageEngine Exchange Reporter Plus through 5721 are vulnerable to ReDOS vulnerability in the search module.	4.3	More Details
CVE-2025-64357	Cross-Site Request Forgery (CSRF) vulnerability in Younes JFR. Advanced Database Cleaner advanced-database-cleaner allows Cross Site Request Forgery.This issue affects Advanced Database Cleaner: from n/a through <= 3.1.6.	4.3	More Details
CVE-2025-12156	The Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_post_data() function in versions 2.0.7 to 2.2.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create and publish arbitrary posts.	4.3	More Details
CVE-2025-43493	The issue was addressed with improved checks. This issue is fixed in iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2025-43445	An out-of-bounds read was addressed with improved input validation. This issue is fixed in visionOS 26.1, macOS Sonoma 14.8.2, macOS Sequoia 15.7.2, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	4.3	More Details
CVE-2025-43435	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-43438	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 26.1, iOS 26.1 and iPadOS 26.1, Safari 26.1, visionOS 26.1. Processing maliciously crafted web content may lead to an unexpected Safari crash.	4.3	More Details
CVE-2025-12180	The Qi Blocks plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.4.3. This is due to the plugin storing arbitrary CSS styles submitted via the `qi-blocks/v1/update-styles` REST API endpoint without proper sanitization in the `update_global_styles_callback()` function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary CSS, which can be used to perform actions such as hiding content, overlaying fake UI elements, or exfiltrating sensitive information via CSS injection techniques.	4.3	More Details
CVE-2025-12038	The Folderly plugin for WordPress is vulnerable to unauthorized modification of data due to an insufficient capability check on the /wp-json/folderly/v1/config/clear-all-data REST API endpoint in all versions up to, and including, 0.3. This makes it possible for authenticated attackers, with Author-level access and above, to	4.3	More Details

	clear all data like terms and categories.		
CVE-2025-11983	The WP Discourse plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.5.9. This is due to the plugin unconditionally sending Discourse API credentials (Api-Key and Api-Username headers) to any host specified in a post's discourse_permalink custom field during comment synchronization. This makes it possible for authenticated attackers, with author-level access and above, to exfiltrate sensitive Discourse API credentials to attacker-controlled servers, as well as query internal services and potentially perform further attacks.	4.3	More Details
CVE-2025-11377	The List category posts plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 0.92.0 via the 'catlist' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with contributor-level access and above, to extract data from password protected, private, or draft posts that they should not have access to.	4.3	More Details
CVE-2025-12367	The SiteSEO – SEO Simplified plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.3.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Author-level access and above, to enable or disable arbitrary SiteSEO features that they should not have access to.	4.3	More Details
CVE-2025-43441	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.1 and iPadOS 26.1, tvOS 26.1, Safari 26.1, visionOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-43443	This issue was addressed with improved checks. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-64141	A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus Task Runner Plugin 0.9.2 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2025-11632	The Call Now Button – The #1 Click to Call Button for WordPress plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on multiple functions in all versions up to, and including, 1.5.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to generate links to billing portal, where they can view and modify billing information of the connected, account, generate chat session tokens, view domain status, etc. This vulnerability was partially fixed in version 1.5.4 and fully fixed in version 1.5.5	4.3	More Details
CVE-2025-43458	This issue was addressed through improved state management. This issue is fixed in Safari 26.1, visionOS 26.1, watchOS 26.1, iOS 26.1 and iPadOS 26.1, tvOS 26.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-11587	The Call Now Button – The #1 Click to Call Button for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the activate function in all versions up to, and including, 1.5.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to link the plugin to their nowbuttons.com account and add malicious buttons to the site. The vulnerability is only exploitable on fresh installs where the plugin has not been previously configured with an API key.	4.3	More Details
CVE-2025-20729	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00441512; Issue ID: MSV-4153.	4.2	More Details
CVE-2025-20745	In apusys, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10095441; Issue ID: MSV-4294.	4.2	More Details
CVE-2025-20744	In pda, there is a possible escalation of privilege due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10127160; Issue ID: MSV-4542.	4.2	More Details
CVE-2025-20743	In clkdbg, there is a possible escalation of privilege due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10136671; Issue ID: MSV-4651.	4.2	More Details
CVE-2025-10931	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Umami Analytics allows Cross-Site Scripting (XSS).This issue affects Umami Analytics: from 0.0.0 before 1.0.1.	3.8	More Details
CVE-2025-64350	Missing Authorization vulnerability in Rank Math SEO Rank Math SEO seo-by-rank-math allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Rank Math SEO: from n/a through <= 1.0.252.1.	3.8	More Details

CVE-2025-36249	IBM Jazz for Service Management 1.1.3.0 through 1.1.3.25 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	3.7	More Details
CVE-2025-12616	A vulnerability was detected in PHPGurukul News Portal 1.0. The impacted element is an unknown function of the file /onps/settings.py. Performing manipulation results in insertion of sensitive information into debugging code. It is possible to initiate the attack remotely. The attack's complexity is rated as high. The exploitability is regarded as difficult. The exploit is now public and may be used.	3.7	More Details
CVE-2025-12547	A vulnerability was identified in LogicalDOC Community Edition up to 9.2.1. This vulnerability affects unknown code of the file /login.jsp of the component Admin Login Page. Such manipulation leads to improper restriction of excessive authentication attempts. The attack can be executed remotely. This attack is characterized by high complexity. It is stated that the exploitability is difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-10636	The NS Maintenance Mode for WP WordPress plugin through 1.3.1 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).	3.5	More Details
CVE-2025-12546	A vulnerability was determined in LogicalDOC Community Edition up to 9.2.1. This affects an unknown part of the component API Key creation UI. This manipulation causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-43395	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An app may be able to access protected user data.	3.3	More Details
CVE-2025-23050	QLowEnergyController in Qt before 6.8.2 mishandles malformed Bluetooth ATT commands, leading to an out-of-bounds read (or division by zero). This is fixed in 5.15.19, 6.5.9, and 6.8.2.	3.1	More Details
CVE-2025-12623	A vulnerability was identified in fushengqian fuint up to 41e26be8a2c609413a0feaa69bdad33a71ae8032. Affected by this issue is some unknown functionality of the file fuint-application/src/main/java/com/fuint/module/clientApi/controller/ClientSignController.java of the component Authentication Token Handler. Such manipulation leads to authorization bypass. The attack may be launched remotely. Attacks of this nature are highly complex. The exploitation is known to be difficult. The exploit is publicly available and might be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	3.1	More Details
CVE-2025-43365	A denial-of-service issue was addressed with improved input validation. This issue is fixed in iOS 26 and iPadOS 26. An unprivileged process may be able to terminate a root processes.	2.8	More Details
CVE-2025-64352	Missing Authorization vulnerability in WPDeveloper Essential Addons for Elementor essential-addons-for-elementor-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Essential Addons for Elementor: from n/a through <= 6.2.4.	2.7	More Details
CVE-2025-43408	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.8.2, macOS Sequoia 15.7.2. An attacker with physical access may be able to access contacts from the lock screen.	2.4	More Details
CVE-2025-43309	A logic issue was addressed with improved checks. This issue is fixed in iOS 26 and iPadOS 26. An attacker with physical access to an iOS device may be able to view notification contents from the Lock Screen.	2.4	More Details
CVE-2025-43423	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 26.1 and iPadOS 26.1, macOS Sequoia 15.7.2, visionOS 26.1. An attacker with physical access to an unlocked device paired with a Mac may be able to view sensitive user information in system logging.	2.0	More Details
CVE-2025-62776	The installer of WTW EAGLE (for Windows) 3.0.8.0 contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with the privileges of the running application.	N/A	More Details
CVE-2025-64162	Rejected reason: Not used	N/A	More Details
CVE-2025-64159	Rejected reason: Not used	N/A	More Details

CVE-2025-47776	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Due to incorrect use of loose (==) instead of strict (===) comparison in the authentication code in versions 2.27.1 and below.PHP type juggling will cause certain MD5 hashes matching scientific notation to be interpreted as numbers. Instances using the MD5 login method allow an attacker who knows the victim's username and has access to an account with a password hash that evaluates to zero to log in without knowing the victim's actual password, by using any other password with a hash that also evaluates to zero This issue is fixed in version 2.27.2.	N/A	More Details
CVE-2025-12461	This vulnerability allows an attacker to access parts of the application that are not protected by any type of access control. The attacker could access this path '…/epsilonnet/License/About.aspx' and obtain information on both the licence and the configuration of the product by knowing which modules are installed.	N/A	More Details
CVE-2025-48076	Galette is a membership management web application for non profit organizations. Versions 1.1.5.2 and below allow a user to edit a group name and insert an XSS payload. This issue is fixed in version 1.2.0.	N/A	More Details
CVE-2025-48884	Galette is a membership management web application for non profit organizations. In versions 1.1.5.2 and below, Galette's Document Type is vulnerable to Cross-site Scripting. This issue is fixed in version 1.2.0.	N/A	More Details
CVE-2025-62507	Redis is an open source, in-memory database that persists on disk. In versions 8.2.0 and above, a user can run the XACKDEL command with multiple ID's and trigger a stack buffer overflow, which may potentially lead to remote code execution. This issue is fixed in version 8.2.3. To workaround this issue without patching the redis-server executable is to prevent users from executing XACKDEL operation. This can be done using ACL to restrict XACKDEL command.	N/A	More Details
CVE-2025-64161	Rejected reason: Not used	N/A	More Details
CVE-2025-64160	Rejected reason: Not used	N/A	More Details
CVE-2025-62520	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions 2.27.1 and below, due to insufficient access-level checks, any non-admin user with access to manage_config_columns_page.php can use the Copy From action to retrieve the columns configuration from a private project they have no access to. This issue is fixed in version 2.27.2.	N/A	More Details
CVE-2025-62715	ClipBucket v5 is an open source video sharing platform. Versions 5.5.2-#147 and below contain a stored Cross-Site Scripting (XSS) vulnerability in ClipBucket's Collection tags feature. An authenticated normal user can create a tag containing HTML or JavaScript, which is later rendered unescaped in collection detail and tag-list pages. As a result, arbitrary JavaScript executes in the browsers of all users who view the affected pages. This issue is fixed in version 5.5.2-#152.	N/A	More Details
CVE-2025-62719	LinkAce is a self-hosted archive to collect website links. In versions 2.3.0 and below, the htmlKeywordsFromUrl function in the FetchController class accepts user-provided URLs and makes HTTP requests to them without validating that the destination is not an internal or private network resource. This Server-Side Request Forgery (SSRF) vulnerability allows authenticated attackers to use the application server to perform port scanning and service discovery on internal networks. Practical impact is very limited because the function only extracts content from HTML meta keywords tags, which prevents meaningful data exfiltration from databases, APIs, or cloud metadata endpoints. This issue is fixed in version 2.4.0.	N/A	More Details
CVE-2025-62722	LinkAce is a self-hosted archive to collect website links. In versions 2.3.1 and below, the social media sharing functionality contains a Stored Cross-Site Scripting (XSS) vulnerability that allows any authenticated user to inject arbitrary JavaScript by creating a link with malicious HTML in the title field. When a user views the link details page and the shareable links are rendered, the malicious JavaScript executes in their browser. This vulnerability affects multiple sharing services and can be exploited to steal session cookies, perform actions on behalf of users, or deliver malware. This issue is fixed in version 2.4.0.	N/A	More Details
CVE-2025-59596	CVE-2025-59596 is a denial-of-service vulnerability in Secure Access Windows client versions 12.0 to 14.10 that is addressed in version 14.12. If a local networking policy is active, attackers on an adjacent network may be able to send a crafted packet and cause the client system to crash.	N/A	More Details
CVE-2025-62721	LinkAce is a self-hosted archive to collect website links. In versions 2.3.1 and below, authenticated RSS feed endpoints in the FeedController class fail to implement proper authorization checks, allowing any authenticated user to access all links, lists, and tags from all users in the system, regardless of their ownership or visibility settings. This issue is fixed in version 2.4.0.	N/A	More Details
CVE-2025-59595	CVE-2025-59595 is an internally discovered denial of service vulnerability in versions of Secure Access prior to 14.12. An attacker can send a specially crafted packet to a server in a non-default configuration and cause the server to crash.	N/A	More Details
	LinkAce is a self-hosted archive to collect website links. Versions 2.3.1 and below allow any authenticated		

CVE-2025-62720	user to export the entire database of links from all users in the system, including private links that should only be accessible to their owners. The HTML and CSV export functions in the ExportController class retrieve all links without applying any ownership or visibility filtering, effectively bypassing all access controls implemented elsewhere in the application. This issue is fixed in version 2.4.0.	N/A	More Details
CVE-2025-41341	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameters 'id_denuncia' and 'seguro' in '/backend/api/buscarUsuarioByDenuncia.php'.	N/A	More Details
CVE-2025-12058	The Keras.Model.load_model method, including when executed with the intended security mitigation safe_mode=True, is vulnerable to arbitrary local file loading and Server-Side Request Forgery (SSRF). This vulnerability stems from the way the StringLookup layer is handled during model loading from a specially crafted .keras archive. The constructor for the StringLookup layer accepts a vocabulary argument that can specify a local file path or a remote file path. * Arbitrary Local File Read: An attacker can create a malicious .keras file that embeds a local path in the StringLookup layer's configuration. When the model is loaded, Keras will attempt to read the content of the specified local file and incorporate it into the model state (e.g., retrievable via get_vocabulary()), allowing an attacker to read arbitrary local files on the hosting system. * Server-Side Request Forgery (SSRF): Keras utilizes tf.io.gfile for file operations. Since tf.io.gfile supports remote filesystem handlers (such as GCS and HDFS) and HTTP/HTTPS protocols, the same mechanism can be leveraged to fetch content from arbitrary network endpoints on the server's behalf, resulting in an SSRF condition. The security issue is that the feature allowing external path loading was not properly restricted by the safe_mode=True flag, which was intended to prevent such unintended data access.	N/A	More Details
CVE-2025-41113	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'id_denuncia' in '/backend/api/buscarDenunciaByPin.php'.	N/A	More Details
CVE-2023-7324	In the Linux kernel, the following vulnerability has been resolved: scsi: ses: Fix possible addl_desc_ptr out-of-bounds accesses Sanitize possible addl_desc_ptr out-of-bounds accesses in ses_enclosure_data_process().	N/A	More Details
CVE-2025-40083	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_qfq: Fix null-deref in agg_dequeue To prevent a potential crash in agg_dequeue (net/sched/sch_qfq.c) when cl->qdisc->ops->peek(cl->qdisc) returns NULL, we check the return value before using it, similar to the existing approach in sch_hfsc.c. To avoid code duplication, the following changes are made: 1. Changed qdisc_warn_nonwc(include/net/pkt_sched.h) into a static inline function. 2. Moved qdisc_peek_len from net/sched/sch_hfsc.c to include/net/pkt_sched.h so that sch_qfq can reuse it. 3. Applied qdisc_peek_len in agg_dequeue to avoid crashing.	N/A	More Details
CVE-2025-40084	In the Linux kernel, the following vulnerability has been resolved: ksmbd: transport_ipc: validate payload size before reading handle handle_response() dereferences the payload as a 4-byte handle without verifying that the declared payload size is at least 4 bytes. A malformed or truncated message from ksmbd.mountd can lead to a 4-byte read past the declared payload size. Validate the size before dereferencing. This is a minimal fix to guard the initial handle read.	N/A	More Details
CVE-2025-40085	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix NULL pointer deference in try_to_register_card In try_to_register_card(), the return value of usb_ifnum_to_if() is passed directly to usb_interface_claimed() without a NULL check, which will lead to a NULL pointer dereference when creating an invalid USB audio device. Fix this by adding a check to ensure the interface pointer is valid before passing it to usb_interface_claimed().	N/A	More Details
CVE-2023-39178	Rejected reason: Duplicate of CVE-2023-52441.	N/A	More Details
CVE-2023-39177	Rejected reason: Duplicate of CVE-2023-52442.	N/A	More Details
CVE-2025-12683	The service employed by Everything, running as SYSTEM, communicates with the lower privileged Everything GUI via a named pipe. The named pipe has a NULL DACL and thus provides all users full permission over it; leading to potential Service Denial Of Service or Privilege escalation(only if chained with other elements) for a local low privilege user.	N/A	More Details
CVE-2025-41111	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'id_denuncia' in '/backend/api/buscarComentariosByDenuncia.php'.	N/A	More Details
CVE-2025-41112	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'web' in '/backend/api/buscarConfiguracionParametros2.php'.	N/A	More Details

CVE-2025-41114	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameters 'id_denuncia' and 'id_user' in '/backend/api/buscarDocumentosByIdDenunciaUsuario.php'.	N/A	More Details
CVE-2025-12108	The Survision LPR Camera system does not enforce password protection by default. This allows access to the configuration wizard immediately without a login prompt or credentials check.	N/A	More Details
CVE-2025-41335	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameters 'id' and ' 'id_sociedad' in '/api/buscarEmpresaById.php'.	N/A	More Details
CVE-2025-41337	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'web' in '/backend/api/buscarSSOParametros.php'.	N/A	More Details
CVE-2025-41338	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameters 'id_denuncia' and 'id_user' in '/backend/api/buscarTestigoByIdDenunciaUsuario.php'.	N/A	More Details
CVE-2025-41339	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'id_sociedad' in '/backend/api/buscarTipoDenuncia.php'.	N/A	More Details
CVE-2025-41340	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameters 'id_tp_denuncia' and 'id_sociedad' in '/backend/api/buscarTipoDenunciabyId.php'.	N/A	More Details
CVE-2025-41342	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'id_user' in '/backend/api/buscarUsuarioId.php'.	N/A	More Details
CVE-2025-41343	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'email' in '/backend/api/users/searchUserByEmail.php'.	N/A	More Details
CVE-2025-41344	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'id_archivo' in '/backend/api/verArchivo.php'.	N/A	More Details
CVE-2025-41345	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameters 'id_denuncia' and 'id_user' in '/backend/api/buscarDenunciasById.php'.	N/A	More Details
CVE-2025-41336	A lack of authorisation vulnerability has been detected in CanalDenuncia.app. This vulnerability allows an attacker to access other users' information by sending a POST through the parameter 'web' in '/backend/api/buscarConfiguracionParametros.php'.	N/A	More Details
CVE-2025-40086	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Don't allow evicting of BOs in same VM in array of VM binds An array of VM binds can potentially evict other buffer objects (BOs) within the same VM under certain conditions, which may lead to NULL pointer dereferences later in the bind pipeline. To prevent this, clear the allow_res_evict flag in the xe_bo_validate call. v2: - Invert polarity of no_res_evict (Thomas) - Add comment in code explaining issue (Thomas) (cherry picked from commit 8b9ba8d6d95fe75fed6b0480bb03da4b321bea08)	N/A	More Details
CVE-2025-43376	A logic issue was addressed with improved state management. This issue is fixed in Safari 26, tvOS 26, watchOS 26, iOS 26 and iPadOS 26, visionOS 26. A remote attacker may be able to view leaked DNS queries with Private Relay turned on.	N/A	More Details
CVE-2020-36862	Nagios XI versions prior to 5.6.11 contain unauthenticated vulnerabilities in the Highcharts local exporting tool. Crafted export requests could (1) inject script into exported/returned content due to insufficient output encoding (XSS), and (2) cause the server to fetch attacker-specified URLs (SSRF), potentially accessing internal network resources. An unauthenticated remote attacker can leverage these issues to execute script in a user's browser when the exported content is viewed and to disclose sensitive information reachable from the export server via SSRF.	N/A	More Details
CVE-2021-47691	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.1 / Nagios XI 5.8.2 contains multiple cross-site scripting (XSS) vulnerabilities via the Services page affecting the config_name and service_description fields. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2021-	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.1 / Nagios XI 5.8.2 contains multiple cross-site scripting (XSS) vulnerabilities in Overlay modals. Insufficient validation or escaping of user-supplied	N/A	More

47690	input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.		Details
CVE-2021-47689	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.0 / Nagios XI 5.8.0 contais a cross-site scripting (XSS) vulnerability in the Templates pages, specifically in the UI logic that renders and handles the Active/Actions buttons. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2020-36869	Nagios XI versions prior to 5.7.5 contain a SQL injection vulnerability in the SNMP Trap Interface edit page. Exploitation requires an account with administrative privileges to access the affected interface. A user with administrative access could supply crafted input that is not properly sanitized, allowing SQL injection that may lead to unauthorized disclosure or modification of application data or execution of arbitrary SQL commands against the backend database.	N/A	More Details
CVE-2020-36868	Nagios XI versions prior to 5.7.3 contain a privilege escalation vulnerability in the getprofile.sh helper script. The script performed profile retrieval and initialization routines using insecure file/command handling and insufficient validation of attacker-controlled inputs, and in some deployments executed with elevated privileges. A local attacker with low-level access could exploit these weaknesses to cause the script to execute arbitrary commands or modify privileged files, resulting in privilege escalation.	N/A	More Details
CVE-2020-36867	Nagios XI versions prior to 5.7.3 contain a command injection vulnerability in the report PDF download/export functionality. User-supplied values used in the PDF generation pipeline or the wrapper that invokes offline/pdf helper utilities were insufficiently validated or improperly escaped, allowing an authenticated attacker who can trigger PDF exports to inject shell metacharacters or arguments.	N/A	More Details
CVE-2020-36866	Nagios XI versions prior to 5.7.2 are vulnerable to cross-site scripting (XSS) via the Manage Users page of the Admin interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2020-36865	Nagios XI versions prior to 5.7.2 are vulnerable to cross-site scripting (XSS) via the BPI (Business Process Intelligence) component’s Config Management and Edit Config page. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2020-36864	Nagios XI versions prior to 5.7.2 are vulnerable to cross-site scripting (XSS) via the background color settings in Dashboards. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2020-36863	Nagios XI versions prior to 5.7.2 allow PHP files to be uploaded to the Audio Import directory and executed from that location. The upload handler did not properly restrict file types or enforce storage outside of the webroot, and the web server permitted execution within the upload directory. An authenticated attacker with access to the audio import feature could upload a crafted PHP file and then request it to achieve remote code execution with the privileges of the application service.	N/A	More Details
CVE-2020-36861	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.0.8 / Nagios XI 5.7.5 contains multiple cross-site scripting (XSS) vulnerabilities in the overlay UI elements and the Notification/Check Period pages. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2021-47693	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.3 / Nagios XI 5.8.5 contains a SQL injection vulnerability in the search text handling. Unsanitized user-supplied input was incorporated into SQL queries used by configuration object editors, allowing authenticated users to inject SQL fragments. Successful exploitation could lead to unauthorized disclosure or modification of configuration and application data, and in some environments could allow further compromise of the application or backend database.	N/A	More Details
CVE-2020-36860	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.0.7 / Nagios XI 5.7.4 contains multiple cross-site scripting (XSS) vulnerabilities in the object edit pages. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2020-36859	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.0.7 / Nagios XI 5.7.4 contains multiple SQL injection vulnerabilities in the object edit pages. Unsanitized user-supplied input was incorporated into SQL queries used by configuration object editors, allowing authenticated users to inject SQL fragments. Successful exploitation could lead to unauthorized disclosure or modification of configuration and application data, and in some environments could allow further compromise of the application or backend database.	N/A	More Details
CVE-2020-36858	Nagios Log Server versions prior to 2.1.6 contain cross-site scripting (XSS) vulnerabilities via the web interface on the Create User, Edit User, and Manage Host Lists pages. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-	Nagios XI versions prior to 5.6.14 contain a post-authentication SQL injection vulnerability in the SNMP Trap Interface page. Exploitation requires an account with administrative privileges to access the affected		

2020-36857	interface. A user with administrative access could supply crafted input that is not properly sanitized, allowing SQL injection that may lead to unauthorized disclosure or modification of application data or execution of arbitrary SQL commands against the backend database.	N/A	More Details
CVE-2020-36856	Nagios XI versions prior to 5.6.14 contain an authenticated remote command execution vulnerability in the CCM command_test.php script. Insufficient validation of the `address` parameter allows an authenticated user with access to the Core Config Manager to inject shell metacharacters that are incorporated into backend command invocations. Successful exploitation enables arbitrary command execution with the privileges of the Nagios XI web application user and may be leveraged to execute commands on the underlying XI host, modify system configuration, or fully compromise the host.	N/A	More Details
CVE-2018-25123	Nagios XI versions prior to 5.5.7 contain a privilege escalation vulnerability in the MRTG graphing component. MRTG-related processes/scripts executed with excessive privileges, allowing a local attacker with limited system access to abuse file/command execution paths or writable resources to gain elevated privileges.	N/A	More Details
CVE-2018-25122	Nagios XI versions prior to 5.4.13 contain a remote code execution vulnerability in the Component Download page. The download/import handler used unsafe command construction with attacker-controlled input and lacked sufficient validation and output encoding, allowing an authenticated user to inject commands or otherwise execute arbitrary code with the privileges of the application service.	N/A	More Details
CVE-2018-25121	Nagios XI versions prior to 5.4.13 are vulnerable to cross-site scripting (XSS) via the Views page of the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2018-25119	Nagios Fusion versions prior to 4.1.5 are vulnerable to cross-site scripting (XSS) via the "fusionwindow" parameter. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2017-20209	Nagios Fusion versions prior to 4.0.1 are vulnerable to cross-site scripting (XSS) via the Users and Servers pages. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2021-47692	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. It has been identified as a duplicate of https://www.cve.org/CVERecord?id=CVE-2021-33179 .	N/A	More Details
CVE-2021-47694	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.4 / Nagios XI 5.8.6 contains a reflected cross-site scripting (XSS) vulnerability via the Test Command functionality. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2016-15052	Nagios XI versions prior to 5.2.4 are vulnerable to cross-site scripting (XSS) via the Menu System of the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-53689	Nagios Fusion versions prior to 4.2.0 contain a reflected cross-site scripting (XSS) vulnerability in the license key configuration flow that can result in execution of attacker-controlled script in the browser of a user who follows a crafted URL. While the application server itself is not directly corrupted by the reflected XSS, the resulting browser compromise can lead to credential/session theft and unauthorized administrative actions.	N/A	More Details
CVE-2023-7321	Nagios Log Server versions prior to 2.1.14 are vulnerable to cross-site scripting (XSS) via the Snapshots Page. Untrusted log content was not safely encoded for the output context, allowing attacker-controlled data present in logs to execute script in the victim’s browser within the application origin.	N/A	More Details
CVE-2023-7319	Nagios Network Analyzer versions prior to 2024R1 are vulnerable to cross-site scripting (XSS) via the Percentile Calculator menu. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-7318	Nagios XI versions prior to < 2024R1.0.2 are vulnerable to cross-site scripting (XSS) via the Nagios Core Command Expansion page. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-7317	Nagios XI versions prior to 2024R1 contain a missing access control vulnerability via the Web SSH Terminal. A remote, low-privileged attacker could access or interact with the terminal interface without sufficient authorization, potentially allowing unauthorized command execution or disclosure of sensitive information.	N/A	More Details
CVE-2023-7316	Nagios XI versions prior to 2024R1 are vulnerable to cross-site scripting (XSS) via the Graph Explorer component. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-7315	Nagios XI versions prior to 5.11.3 are vulnerable to cross-site scripting (XSS) via the Graph Explorer component. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details

CVE-2023-7314	Nagios XI versions prior to 5.11.3 are vulnerable to cross-site scripting (XSS) via the Bandwidth Report component. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-7313	Nagios XI versions prior to 5.11.3 are vulnerable to cross-site scripting (XSS) via the Bulk Modifications tool. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-7312	Nagios Fusion versions prior to 4.2.0 contain a stored cross-site scripting (XSS) vulnerability when adding or configuring Email Settings. Unsanitized user input can be stored and later rendered in the administrative UI, causing JavaScript to execute in the browser of any user who views the affected page. An attacker who can add or modify SMTP/email settings or manipulate the sendmail configuration fields could persist a malicious payload that executes in the context of other users' browsers.	N/A	More Details
CVE-2023-53690	Nagios Fusion versions prior to 4.2.0 contain a stored cross-site scripting (XSS) vulnerability in the LDAP/AD authentication-server configuration. Unsanitized user input can be stored and later rendered in the administrative UI, causing JavaScript to execute in the browser of any user who views the affected page. An attacker who can add authentication servers via LDAP/AD integration could persist a malicious payload that executes in the context of other users' browsers.	N/A	More Details
CVE-2023-53688	Nagios XI versions prior to 5.11.3 are vulnerable to cross-site scripting (XSS) and cross-site request forgery (CSRF) via the Hypermap Replay component. An attacker can submit crafted input that is not properly validated or escaped, allowing injection of malicious script that executes in the context of a victim's browser (XSS). Additionally, the component does not enforce sufficient anti-CSRF protections on state-changing operations, enabling an attacker to induce authenticated users to perform unwanted actions.	N/A	More Details
CVE-2021-47695	Nagios XI versions prior to 5.8.0 are vulnerable to stored cross-site scripting (XSS) via the My Tools page. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2022-50588	Nagios XI versions prior to 5.8.9 are vulnerable to cross-site scripting (XSS) in the update checking feature. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2022-50587	Nagios XI versions prior to 5.8.9 are vulnerable to cross-site scripting (XSS) via the Apply Configuration error text. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2022-50586	Nagios XI versions prior to 5.8.9 are vulnerable to cross-site scripting (XSS) in the BPI component via the info URL field. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2022-50585	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.7 / Nagios XI 5.8.9 contains a cross-site scripting (XSS) vulnerability via the Audit Log page search input. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2022-50584	The Core Config Manager (CCM) in Nagios XI versions prior to CCM 3.1.6 / Nagios XI 5.8.8 contains a cross-site scripting (XSS) vulnerability via the search and deletion interfaces. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2021-4461	Seeyon Zhiyuan OA Web Application System versions up to and including 7.0 SP1 improperly decode and parse the `enc` parameter in thirdpartyController.do. The decoded map values can influence session attributes without sufficient authentication/authorization checks, enabling attackers to assign a session to arbitrary user IDs. VulnCheck has observed this vulnerability being exploited in the wild as of 2025-10-30 at 00:30:40.855917 UTC.	N/A	More Details
CVE-2021-47700	Nagios XI versions prior to 5.8.7 used a temporary directory for Highcharts exports with overly permissive ownership/permissions under the Apache user. Local or co-hosted processes could read/overwrite export artifacts or manipulate paths, risking disclosure or tampering and potential code execution depending on deployment.	N/A	More Details
CVE-2021-47699	Nagios XI versions prior to 5.8.7 are vulnerable to cross-site scripting (XSS) via the Audit Log page’s Send to NLS form. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2021-47697	Nagios XI versions prior to 5.8.0 are vulnerable to cross-site scripting (XSS) via the Views feature URL handling. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2021-	Nagios XI versions prior to 5.8.0 are vulnerable to cross-site scripting (XSS) via BPI config ID handling. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary	N/A	More

47696	script in the context of a victim's browser.		Details
CVE-2016-15053	Nagios XI versions prior to 5.2.4 are vulnerable to cross-site scripting (XSS) via the “My Reports” listing of the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2016-15051	Nagios XI versions prior to 5.2.4 are vulnerable to cross-site scripting (XSS) via the Reports interface through values from the startdate and enddate fields. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2025-34501	Deck Mate 2 is distributed with static, hard-coded credentials for the root shell and web user interface, while multiple management services (SSH, HTTP, Telnet, SMB, X11) are enabled by default. If an attacker can reach these interfaces - most often through local or near-local access such as connecting to the USB or Ethernet ports beneath the table - the built-in credentials permit administrative login and full control of the system. Once authenticated, an attacker can access firmware utilities, modify controller software, and establish persistent compromise. Remote attack paths via network, cellular, or telemetry links may exist in specific configurations but generally require additional capabilities or operator error. The vendor reports that USB access has been disabled in current firmware builds.	N/A	More Details
CVE-2025-40099	In the Linux kernel, the following vulnerability has been resolved: cifs: parse_dfs_referrals: prevent oob on malformed input Malicious SMB server can send invalid reply to FSCTL_DFS_GET_REFERRALS - reply smaller than sizeof(struct get_dfs_referral_rsp) - reply with number of referrals smaller than NumberOfReferrals in the header Processing of such replies will cause oob. Return -EINVAL error on such replies to prevent oob-s.	N/A	More Details
CVE-2025-10317	Quick.Cart is vulnerable to Cross-Site Request Forgery in product creation functionality. Malicious attacker can craft special website, which when visited by the admin, will automatically send a POST request creating a malicious product with content defined by the attacker. This software does not implement any protection against this type of attack. All forms available in this software are potentially vulnerable. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.7 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-53883	A Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability allows attackers to run arbitrary javascript via a reflected XSS issue in the search fields.This issue affects Container suse/manager/5.0/x86_64/server:latest: from ? before 5.0.28-150600.3.36.8; SUSE Manager Server LTS 4.3: from ? before 4.3.88-150400.3.113.5.	N/A	More Details
CVE-2025-53880	A Path Traversal vulnerability in the tftpsync/add and tftpsync/delete scripts allows a remote attacker on an adjacent network to write or delete files on the filesystem with the privileges of the unprivileged wwwrun user. Although the endpoint is unauthenticated, access is restricted to a list of allowed IP addresses.	N/A	More Details
CVE-2025-39663	Cross-Site Scripting (XSS) vulnerability in Checkmk's distributed monitoring allows a compromised remote site to inject malicious HTML code into service outputs in the central site. Affecting Checkmk before 2.4.0p14, 2.3.0p39, 2.2.0 and 2.1.0 (eol).	N/A	More Details
CVE-2025-40105	In the Linux kernel, the following vulnerability has been resolved: vfs: Don't leak disconnected dentries on umount When user calls open_by_handle_at() on some inode that is not cached, we will create disconnected dentry for it. If such dentry is a directory, exportfs_decode_fh_raw() will then try to connect this dentry to the dentry tree through reconnect_path(). It may happen for various reasons (such as corrupted fs or race with rename) that the call to lookup_one_unlocked() in reconnect_one() will fail to find the dentry we are trying to reconnect and instead create a new dentry under the parent. Now this dentry will not be marked as disconnected although the parent still may well be disconnected (at least in case this inconsistency happened because the fs is corrupted and .. doesn't point to the real parent directory). This creates inconsistency in disconnected flags but AFAICS it was mostly harmless. At least until commit f1ee616214cb ("VFS: don't keep disconnected dentries on d_anon") which removed adding of most disconnected dentries to sb->s_anon list. Thus after this commit cleanup of disconnected dentries implicitely relies on the fact that dput() will immediately reclaim such dentries. However when some leaf dentry isn't marked as disconnected, as in the scenario described above, the reclaim doesn't happen and the dentries are "leaked". Memory reclaim can eventually reclaim them but otherwise they stay in memory and if umount comes first, we hit infamous "Busy inodes after unmount" bug. Make sure all dentries created under a disconnected parent are marked as disconnected as well.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: ixgbevf: fix mailbox API compatibility by negotiating supported features There was backward compatibility in the terms of mailbox API. Various drivers from various OSes supporting 10G adapters from Intel portfolio could easily negotiate mailbox API. This convention has been broken since introducing API 1.4. Commit 0062e7cc955e ("ixgbevf: add VF IPsec offload code") added support for IPSec which is specific only for the kernel ixgbe driver. None of the rest of the Intel 10G PF/VF drivers supports it. And actually lack of support was not included in the IPSec implementation - there were no such code paths. No possibility to negotiate support for the feature was introduced along with introduction of the feature itself. Commit 339f28964147 ("ixgbevf: Add support for new mailbox communication between PF and VF") increasing API version to 1.5 did the same - it introduced code supported specifically by the PF ESX driver. It altered API version for the VF driver in the same time not		

2025-40104	touching the version defined for the PF ixgbe driver. It led to additional discrepancies, as the code provided within API 1.6 cannot be supported for Linux ixgbe driver as it causes crashes. The issue was noticed some time ago and mitigated by Jake within the commit d0725312adf5 ("ixgbevf: stop attempting IPSEC offload on Mailbox API 1.5"). As a result we have regression for IPsec support and after increasing API to version 1.6 ixgbevf driver stopped to support ESX MBX. To fix this mess add new mailbox op asking PF driver about supported features. Basing on a response determine whether to set support for IPSec and ESX-specific enhanced mailbox. New mailbox op, for compatibility purposes, must be added within new API revision, as API version of OOT PF & VF drivers is already increased to 1.6 and doesn't incorporate features negotiate op. Features negotiation mechanism gives possibility to be extended with new features when needed in the future.	N/A	More Details
CVE-2025-40103	In the Linux kernel, the following vulnerability has been resolved: smb: client: Fix refcount leak for cifs_sb_tlink Fix three refcount inconsistency issues related to `cifs_sb_tlink`. Comments for `cifs_sb_tlink` state that `cifs_put_tlink()` needs to be called after successful calls to `cifs_sb_tlink()`. Three calls fail to update refcount accordingly, leading to possible resource leaks.	N/A	More Details
CVE-2025-40102	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Prevent access to vCPU events before init Another day, another syzkaller bug. KVM erroneously allows userspace to pend vCPU events for a vCPU that hasn't been initialized yet, leading to KVM interpreting a bunch of uninitialized garbage for routing / injecting the exception. In one case the injection code and the hyp disagree on whether the vCPU has a 32bit EL1 and put the vCPU into an illegal mode for AArch64, tripping the BUG() in exception_target_el() during the next injection: kernel BUG at arch/arm64/kvm/inject_fault.c:40! Internal error: Oops - BUG: 00000000f2000800 [#1] SMP CPU: 3 UID: 0 PID: 318 Comm: repro Not tainted 6.17.0-rc4-00104-g10fd0285305d #6 PREEMPT Hardware name: linux,dummy-virt (DT) pstate: 21402009 (nzCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) pc : exception_target_el+0x88/0x8c lr : pend_serror_exception+0x18/0x13c sp : ffff800082f03a10 x29: ffff800082f03a10 x28: ffff0000cb132280 x27: 0000000000000000 x26: 0000000000000000 x25: ffff0000c2a99c20 x24: 0000000000000000 x23: 0000000000008000 x22: 0000000000000002 x21: 0000000000000004 x20: 0000000000008000 x19: ffff0000c2a99c20 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 00000000200000c0 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : ffff800082f03af8 x7 : 0000000000000000 x6 : 0000000000000000 x5 : ffff800080f621f0 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 000000000040009b x1 : 0000000000000003 x0 : ffff0000c2a99c20 Call trace: exception_target_el+0x88/0x8c (P) kvm_inject_serror_esr+0x40/0x3b4 __kvm_arm_vcpu_set_events+0xf0/0x100 kvm_arch_vcpu_ioctl+0x180/0x9d4 kvm_vcpu_ioctl+0x60c/0x9f4 __arm64_sys_ioctl+0xac/0x104 invoke_syscall+0x48/0x110 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xf0 el0t_64_sync_handler+0xa0/0xe4 el0t_64_sync+0x198/0x19c Code: f946bc01 b4fffe61 9101e020 17fffff2 (d4210000) Reject the ioctls outright as no sane VMM would call these before KVM_ARM_VCPU_INIT anyway. Even if it did the exception would've been thrown away by the eventual reset of the vCPU's state.	N/A	More Details
CVE-2025-40101	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix memory leaks when rejecting a non SINGLE data profile without an RST At the end of btrfs_load_block_group_zone_info() the first thing we do is to ensure that if the mapping type is not a SINGLE one and there is no RAID stripe tree, then we return early with an error. Doing that, though, prevents the code from running the last calls from this function which are about freeing memory allocated during its run. Hence, in this case, instead of returning early, we set the ret value and fall through the rest of the cleanup code.	N/A	More Details
CVE-2025-40100	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not assert we found block group item when creating free space tree Currently, when building a free space tree at populate_free_space_tree(), if we are not using the block group tree feature, we always expect to find block group items (either extent items or a block group item with key type BTRFS_BLOCK_GROUP_ITEM_KEY) when we search the extent tree with btrfs_search_slot_for_read(), so we assert that we found an item. However this expectation is wrong since we can have a new block group created in the current transaction which is still empty and for which we still have not added the block group's item to the extent tree, in which case we do not have any items in the extent tree associated to the block group. The insertion of a new block group's block group item in the extent tree happens at btrfs_create_pending_block_groups() when it calls the helper insert_block_group_item(). This typically is done when a transaction handle is released, committed or when running delayed refs (either as part of a transaction commit or when serving tickets for space reservation if we are low on free space). So remove the assertion at populate_free_space_tree() even when the block group tree feature is not enabled and update the comment to mention this case. Syzbot reported this with the following stack trace: BTRFS info (device loop3 state M): rebuilding free space tree assertion failed: ret == 0 :: 0, in fs/btrfs/free-space-tree.c:1115 ------------[cut here]------------ kernel BUG at fs/btrfs/free-space-tree.c:1115! Oops: invalid opcode: 0000 [#1] SMP KASAN PTI CPU: 1 UID: 0 PID: 6352 Comm: syz.3.25 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/18/2025 RIP: 0010:populate_free_space_tree+0x700/0x710 fs/btrfs/free-space-tree.c:1115 Code: ff ff e8 d3 (...) RSP: 0018:ffffc9000430f780 EFLAGS: 00010246 RAX: 0000000000000043 RBX: ffff88805b709630 RCX: fea61d0e2e79d000 RDX: 0000000000000000 RSI: 0000000080000000 RDI: 0000000000000000 RBP: ffffc9000430f8b0 R08: ffffc9000430f4a7 R09: 1ffff92000861e94 R10: dffffc0000000000 R11: fffff52000861e95 R12: 0000000000000001 R13: 1ffff92000861f00 R14: dffffc0000000000 R15:	N/A	More Details

	0000000000000000 FS: 00007f424d9fe6c0(0000) GS:ffff888125afc000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fd78ad212c0 CR3: 0000000076d68000 CR4: 00000000003526f0 Call Trace: <TASK> btrfs_rebuild_free_space_tree+0x1ba/0x6d0 fs/btrfs/free-space-tree.c:1364 btrfs_start_pre_rw_mount+0x128f/0x1bf0 fs/btrfs/disk-io.c:3062 btrfs_remount_rw fs/btrfs/super.c:1334 [inline] btrfs_reconfigure+0xaed/0x2160 fs/btrfs/super.c:1559 reconfigure_super+0x227/0x890 fs/super.c:1076 do_remount fs/namespace.c:3279 [inline] path_mount+0xd1a/0xfe0 fs/namespace.c:4027 do_mount fs/namespace.c:4048 [inline] __do_sys_mount fs/namespace.c:4236 [inline] __se_sys_mount+0x313/0x410 fs/namespace.c:4213 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f424e39066a Code: d8 64 89 02 (...) RSP: 002b:00007f424d9fde68 EFLAGS: 00000246 ORIG_RAX: 00000000000000a5 RAX: ffffffffffffffda RBX: 00007f424d9fdef0 RCX: 00007f424e39066a RDX: 0000200000000180 RSI: 0000200000000380 RDI: 0000000000000000 RBP: 0000200000000180 R08: 00007f424d9fdef0 R09: 0000000000000020 R10: 0000000000000020 R11: 0000000000000246 R12: 0000200000000380 R13: 00007f424d9fdeb0 R14: 0000000000000000 R15: 00002000000002c0 </TASK> Modules linked in: ---[end trace 0000000000000000]---		
CVE-2025-40098	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: cs35l41: Fix NULL pointer dereference in cs35l41_get_acpi_mute_state() Return value of a function acpi_evaluate_dsm() is dereferenced without checking for NULL, but it is usually checked for this function. acpi_evaluate_dsm() may return NULL, when acpi_evaluate_object() returns acpi_status other than ACPI_SUCCESS, so add a check to prevent the crach. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-11998	The following HP Card Readers B Models (X3D03B & Y7C05B) are potentially vulnerable to information disclosure, allowing prior user identity to be inherited under certain conditions —e.g., when an NFC device (such as a smartphone/smartwatches) is in proximity during a card swipe event.	N/A	More Details
CVE-2025-40097	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda: Fix missing pointer check in hda_component_manager_init function The __component_match_add function may assign the 'matchptr' pointer the value ERR_PTR(-ENOMEM), which will subsequently be dereferenced. The call stack leading to the error looks like this: hda_component_manager_init |-> component_match_add |-> component_match_add_release |-> __component_match_add (... ,**matchptr, ...) |-> *matchptr = ERR_PTR(-ENOMEM); // assign |-> component_master_add_with_match(... match) |-> component_match_realloc(match, match->num); // dereference Add IS_ERR() check to prevent the crash. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-40096	In the Linux kernel, the following vulnerability has been resolved: drm/sched: Fix potential double free in drm_sched_job_add_resv_dependencies When adding dependencies with drm_sched_job_add_dependency(), that function consumes the fence reference both on success and failure, so in the latter case the dma_fence_put() on the error path (xarray failed to expand) is a double free. Interestingly this bug appears to have been present ever since commit ebd5f74255b9 ("drm/sched: Add dependency tracking"), since the code back then looked like this: drm_sched_job_add_implicit_dependencies(): ... for (i = 0; i < fence_count; i++) { ret = drm_sched_job_add_dependency(job, fences[i]); if (ret) break; } for (; i < fence_count; i++) dma_fence_put(fences[i]); Which means for the failing 'i' the dma_fence_put was already a double free. Possibly there were no users at that time, or the test cases were insufficient to hit it. The bug was then only noticed and fixed after commit 9c2ba265352a ("drm/scheduler: use new iterator in drm_sched_job_add_implicit_dependencies v2") landed, with its fixup of commit 4eaf02d6076c ("drm/scheduler: fix drm_sched_job_add_implicit_dependencies"). At that point it was a slightly different flavour of a double free, which commit 963d0b356935 ("drm/scheduler: fix drm_sched_job_add_implicit_dependencies harder") noticed and attempted to fix. But it only moved the double free from happening inside the drm_sched_job_add_dependency(), when releasing the reference not yet obtained, to the caller, when releasing the reference already released by the former in the failure case. As such it is not easy to identify the right target for the fixes tag so lets keep it simple and just continue the chain. While fixing we also improve the comment and explain the reason for taking the reference and not dropping it.	N/A	More Details
CVE-2025-40095	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_rndis: Refactor bind path to use __free() After an bind/unbind cycle, the rndis->notify_req is left stale. If a subsequent bind fails, the unified error label attempts to free this stale request, leading to a NULL pointer dereference when accessing ep->ops->free_request. Refactor the error handling in the bind path to use the __free() automatic cleanup mechanism.	N/A	More Details
CVE-2025-40094	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_acm: Refactor bind path to use __free() After an bind/unbind cycle, the acm->notify_req is left stale. If a subsequent bind fails, the unified error label attempts to free this stale request, leading to a NULL pointer dereference when accessing ep->ops->free_request. Refactor the error handling in the bind path to use the __free() automatic cleanup mechanism. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 Call trace: usb_ep_free_request+0x2c/0xec gs_free_req+0x30/0x44 acm_bind+0x1b8/0x1f4 usb_add_function+0xcc/0x1f0 configfs_composite_bind+0x468/0x588 gadget_bind_driver+0x104/0x270 really_probe+0x190/0x374 __driver_probe_device+0xa0/0x12c driver_probe_device+0x3c/0x218 __device_attach_driver+0x14c/0x188 bus_for_each_drv+0x10c/0x168 __device_attach+0xfc/0x198	N/A	More Details

	device_initial_probe+0x14/0x24 bus_probe_device+0x94/0x11c device_add+0x268/0x48c usb_add_gadget+0x198/0x28c dwc3_gadget_init+0x700/0x858 __dwc3_set_mode+0x3cc/0x664 process_scheduled_works+0x1d8/0x488 worker_thread+0x244/0x334 kthread+0x114/0x1bc ret_from_fork+0x10/0x20		
CVE-2025-40093	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ecm: Refactor bind path to use __free() After an bind/unbind cycle, the ecm->notify_req is left stale. If a subsequent bind fails, the unified error label attempts to free this stale request, leading to a NULL pointer dereference when accessing ep->ops->free_request. Refactor the error handling in the bind path to use the __free() automatic cleanup mechanism.	N/A	More Details
CVE-2025-40092	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ncm: Refactor bind path to use __free() After an bind/unbind cycle, the ncm->notify_req is left stale. If a subsequent bind fails, the unified error label attempts to free this stale request, leading to a NULL pointer dereference when accessing ep->ops->free_request. Refactor the error handling in the bind path to use the __free() automatic cleanup mechanism. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 Call trace: usb_ep_free_request+0x2c/0xec ncm_bind+0x39c/0x3dc usb_add_function+0xcc/0x1f0 configfs_composite_bind+0x468/0x588 gadget_bind_driver+0x104/0x270 really_probe+0x190/0x374 __driver_probe_device+0xa0/0x12c driver_probe_device+0x3c/0x218 __device_attach_driver+0x14c/0x188 bus_for_each_drv+0x10c/0x168 __device_attach+0xfc/0x198 device_initial_probe+0x14/0x24 bus_probe_device+0x94/0x11c device_add+0x268/0x48c usb_add_gadget+0x198/0x28c dwc3_gadget_init+0x700/0x858 __dwc3_set_mode+0x3cc/0x664 process_scheduled_works+0x1d8/0x488 worker_thread+0x244/0x334 kthread+0x114/0x1bc ret_from_fork+0x10/0x20	N/A	More Details
CVE-2025-40091	In the Linux kernel, the following vulnerability has been resolved: ixgbe: fix too early devlink_free() in ixgbe_remove() Since ixgbe_adapter is embedded in devlink, calling devlink_free() prematurely in the ixgbe_remove() path can lead to UAF. Move devlink_free() to the end. KASAN report: BUG: KASAN: use-after-free in ixgbe_reset_interrupt_capability+0x140/0x180 [ixgbe] Read of size 8 at addr ffff0000adf813e0 by task bash/2095 CPU: 1 UID: 0 PID: 2095 Comm: bash Tainted: G S 6.17.0-rc2-tnguy.net-queue+ #1 PREEMPT(full) [...] Call trace: show_stack+0x30/0x90 (C) dump_stack_lvl+0x9c/0xd0 print_address_description.constprop.0+0x90/0x310 print_report+0x104/0x1f0 kasan_report+0x88/0x180 __asan_report_load8_noabort+0x20/0x30 ixgbe_reset_interrupt_capability+0x140/0x180 [ixgbe] ixgbe_clear_interrupt_scheme+0xf8/0x130 [ixgbe] ixgbe_remove+0x2d0/0x8c0 [ixgbe] pci_device_remove+0xa0/0x220 device_remove+0xb8/0x170 device_release_driver_internal+0x318/0x490 device_driver_detach+0x40/0x68 unbind_store+0xec/0x118 drv_attr_store+0x64/0xb8 sysfs_kf_write+0xcc/0x138 kernfs_fop_write_iter+0x294/0x440 new_sync_write+0x1fc/0x588 vfs_write+0x480/0x6a0 ksys_write+0xf0/0x1e0 __arm64_sys_write+0x70/0xc0 invoke_syscall.constprop.0+0xcc/0x280 el0_svc_common.constprop.0+0xa8/0x248 do_el0_svc+0x44/0x68 el0_svc+0x54/0x160 el0t_64_sync_handler+0xa0/0xe8 el0t_64_sync+0x1b0/0x1b8	N/A	More Details
CVE-2025-40090	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix recursive locking in RPC handle list access Since commit 305853cce3794 ("ksmbd: Fix race condition in RPC handle list access"), ksmbd_session_rpc_method() attempts to lock sess->rpc_lock. This causes hung connections / tasks when a client attempts to open a named pipe. Using Samba's rpcclient tool: $ rpcclient //192.168.1.254 -U user%password $ rpcclient $> srvinfo <connection hung here> Kernel side: "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:kworker/0:0 state:D stack:0 pid:5021 tgid:5021 ppid:2 flags:0x00200000 Workqueue: ksmbd-io handle_ksmbd_work Call trace: __schedule from schedule+0x3c/0x58 schedule from schedule_preempt_disabled+0xc/0x10 schedule_preempt_disabled from rwsem_down_read_slowpath+0x1b0/0x1d8 rwsem_down_read_slowpath from down_read+0x28/0x30 down_read from ksmbd_session_rpc_method+0x18/0x3c ksmbd_session_rpc_method from ksmbd_rpc_open+0x34/0x68 ksmbd_rpc_open from ksmbd_session_rpc_open+0x194/0x228 ksmbd_session_rpc_open from create_smb2_pipe+0x8c/0x2c8 create_smb2_pipe from smb2_open+0x10c/0x27ac smb2_open from handle_ksmbd_work+0x238/0x3dc handle_ksmbd_work from process_scheduled_works+0x160/0x25c process_scheduled_works from worker_thread+0x16c/0x1e8 worker_thread from kthread+0xa8/0xb8 kthread from ret_from_fork+0x14/0x38 Exception stack(0x8529ffb0 to 0x8529fff8) The task deadlocks because the lock is already held: ksmbd_session_rpc_open down_write(&sess->rpc_lock) ksmbd_rpc_open ksmbd_session_rpc_method down_read(&sess->rpc_lock) <-- deadlock Adjust ksmbd_session_rpc_method() callers to take the lock when necessary.	N/A	More Details
CVE-2025-40089	In the Linux kernel, the following vulnerability has been resolved: cxl/features: Add check for no entries in cxl_feature_info cxl EDAC calls cxl_feature_info() to get the feature information and if the hardware has no Features support, cxlfs may be passed in as NULL. [51.957498] BUG: kernel NULL pointer dereference, address: 0000000000000008 [51.965571] #PF: supervisor read access in kernel mode [51.971559] #PF: error_code(0x0000) - not-present page [51.977542] PGD 17e4f6067 P4D 0 [51.981384] Oops: Oops: 0000 [#1] SMP NOPTI [51.986300] CPU: 49 UID: 0 PID: 3782 Comm: systemd-udevd Not tainted 6.17.0dj test+ #64 PREEMPT(voluntary) [51.997355] Hardware name: <removed> [52.009790] RIP: 0010:cxl_feature_info+0xa/0x80 [cxl_core] Add a check for cxlfs before dereferencing it and return -EOPNOTSUPP if there is no cxlfs created due to no hardware support.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix slab-out-of-bounds read in hfsplus_strcasecmp() The hfsplus_strcasecmp() logic can trigger the issue: [117.317703][T9855]		

CVE-2025-40088	== [117.318353][T9855] BUG: KASAN: slab-out-of-bounds in hfsplus_strcasecmp+0x1bc/0x490 [117.318991][T9855] Read of size 2 at addr ffff88802160f40c by task repro/9855 [117.319577][T9855] [117.319773][T9855] CPU: 0 UID: 0 PID: 9855 Comm: repro Not tainted 6.17.0-rc6 #33 PREEMPT(full) [117.319780][T9855] Hardware name: QEMU Ubuntu 24.04 PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [117.319783][T9855] Call Trace: [117.319785][T9855] <TASK> [117.319788][T9855] dump_stack_lvl+0x1c1/0x2a0 [117.319795][T9855] ? __virt_addr_valid+0x1c8/0x5c0 [117.319803][T9855] ? __pfx_dump_stack_lvl+0x10/0x10 [117.319808][T9855] ? rcu_is_watching+0x15/0xb0 [117.319816][T9855] ? lock_release+0x4b/0x3e0 [117.319821][T9855] ? __kasan_check_byte+0x12/0x40 [117.319828][T9855] ? __virt_addr_valid+0x1c8/0x5c0 [117.319835][T9855] ? __virt_addr_valid+0x4a5/0x5c0 [117.319842][T9855] print_report+0x17e/0x7e0 [117.319848][T9855] ? __virt_addr_valid+0x1c8/0x5c0 [117.319855][T9855] ? __virt_addr_valid+0x4a5/0x5c0 [117.319862][T9855] ? __phys_addr+0xd3/0x180 [117.319869][T9855] ? hfsplus_strcasecmp+0x1bc/0x490 [117.319876][T9855] kasan_report+0x147/0x180 [117.319882][T9855] ? hfsplus_strcasecmp+0x1bc/0x490 [117.319891][T9855] hfsplus_strcasecmp+0x1bc/0x490 [117.319900][T9855] ? __pfx_hfsplus_cat_case_cmp_key+0x10/0x10 [117.319906][T9855] hfs_find_rec_by_key+0xa9/0x1e0 [117.319913][T9855] __hfsplus_brec_find+0x18e/0x470 [117.319920][T9855] ? __pfx_hfsplus_bnode_find+0x10/0x10 [117.319926][T9855] ? __pfx_hfs_find_rec_by_key+0x10/0x10 [117.319933][T9855] ? __pfx___hfsplus_brec_find+0x10/0x10 [117.319942][T9855] hfsplus_brec_find+0x28f/0x510 [117.319949][T9855] ? __pfx_hfs_find_rec_by_key+0x10/0x10 [117.319956][T9855] ? __pfx_hfsplus_brec_find+0x10/0x10 [117.319963][T9855] ? __kmalloc_noprof+0x2a9/0x510 [117.319969][T9855] ? hfsplus_find_init+0x8c/0x1d0 [117.319976][T9855] hfsplus_brec_read+0x2b/0x120 [117.319983][T9855] hfsplus_lookup+0x2aa/0x890 [117.319990][T9855] ? __pfx_hfsplus_lookup+0x10/0x10 [117.320003][T9855] ? d_alloc_parallel+0x2f0/0x15e0 [117.320008][T9855] ? __lock_acquire+0xaec/0xd80 [117.320013] [T9855] ? __pfx_d_alloc_parallel+0x10/0x10 [117.320019][T9855] ? __raw_spin_lock_init+0x45/0x100 [117.320026][T9855] ? __init_waitqueue_head+0xa9/0x150 [117.320034][T9855] __lookup_slow+0x297/0x3d0 [117.320039][T9855] ? __pfx___lookup_slow+0x10/0x10 [117.320045][T9855] ? down_read+0x1ad/0x2e0 [117.320055][T9855] lookup_slow+0x53/0x70 [117.320065][T9855] walk_component+0x2f0/0x430 [117.320073][T9855] path_lookupat+0x169/0x440 [117.320081][T9855] filename_lookup+0x212/0x590 [117.320089][T9855] ? __pfx_filename_lookup+0x10/0x10 [117.320098][T9855] ? strncpy_from_user+0x150/0x290 [117.320105][T9855] ? getname_flags+0x1e5/0x540 [117.320112][T9855] user_path_at+0x3a/0x60 [117.320117][T9855] __x64_sys_umount+0xee/0x160 [117.320123][T9855] ? __pfx___x64_sys_umount+0x10/0x10 [117.320129][T9855] ? do_syscall_64+0xb7/0x3a0 [117.320135][T9855] ? entry_SYSCALL_64_after_hwframe+0x77/0x7f [117.320141][T9855] ? entry_SYSCALL_64_after_hwframe+0x77/0x7f [117.320145][T9855] do_syscall_64+0xf3/0x3a0 [117.320150][T9855] ? exc_page_fault+0x9f/0xf0 [117.320154][T9855] entry_SYSCALL_64_after_hwframe+0x77/0x7f [117.320158][T9855] RIP: 0033:0x7f7dd7908b07 [117.320163][T9855] Code: 23 0d 00 f7 d8 64 89 01 48 83 c8 ff c3 66 0f 1f 44 00 00 31 f6 e9 09 00 00 00 66 0f 1f 84 00 00 00 08 [117.320167][T9855] RSP: 002b:00007ffd5ebd9698 EFLAGS: 00000202 ---truncated---	N/A	More Details
CVE-2025-10348	URVE Smart Office is vulnerable to Stored XSS in report problem functionality. An attacker with a low-privileged account can upload an SVG file containing a malicious payload, which will be executed when a victim visits the URL of the uploaded resource. The resource is available to anyone without any form of authentication. This issue was fixed in version 1.1.24.	N/A	More Details
CVE-2025-12515	Systemic Internal Server Errors - HTTP 500 ResponseThis issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2016-15050	Nagios XI versions prior to 5.2.4 contain a SQL injection vulnerability in the notification search functionality. User-supplied search parameters were incorporated into SQL statements without adequate parameterization or sanitation, allowing an authenticated user to manipulate database queries. Successful exploitation could disclose or modify notification data and, in some cases, impact the application database more broadly.	N/A	More Details
CVE-2011-10036	Nagios XI versions prior to 2011R1.9 are vulnerable to cross-site scripting (XSS) via the handling of the "backend_url" JavaScript link. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2016-15049	Nagios Log Server versions prior to 1.4.2 are vulnerable to cross-site scripting (XSS) in the Dashboards section when rendering log entries in the Logs table. Untrusted log content was not safely encoded for the output context, allowing attacker-controlled data present in logs to execute script in the victim’s browser within the application origin.	N/A	More Details
CVE-2013-10074	Nagios XI versions prior to 2012R2.6 are vulnerable to cross-site scripting (XSS) via the Tools Menu of the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2013-10073	Nagios XI versions prior to 2012R1.6 contain a shell command injection vulnerability in the Auto-Discovery tool. User-controlled input is passed to a shell without adequate sanitation or argument quoting, allowing an authenticated user with access to discovery functionality to execute arbitrary commands with the privileges of the application service.	N/A	More Details

CVE-2013-10072	Nagios XI versions prior to 2012R1.6 contain an authorization flaw in the Auto-Discovery functionality. Users with read-only roles could directly reach Auto-Discovery endpoints and pages that should require elevated permissions, exposing discovery results and allowing unintended access to discovery operations.	N/A	More Details
CVE-2013-10071	Nagios XI versions prior to 2012R1.6 contain a reflected cross-site scripting (XSS) vulnerability in the dashboard dashlet AJAX load functionality. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2012-10063	Nagios XI versions prior to 2012R1.3 contain a SQL injection vulnerability in the legacy Core Configuration Manager (CCM) interface. Authenticated users could manipulate SQL queries by supplying crafted input to specific CCM parameters, potentially allowing access to configuration data stored in the application database. Successful exploitation could disclose or modify notification data and, in some cases, impact the application database more broadly.	N/A	More Details
CVE-2011-10040	Nagios XI versions prior to 2011R1.9 are vulnerable to cross-site scripting (XSS) via the link-handling functions used by status and report pages. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2011-10039	Nagios XI versions prior to 2011R1.9 are vulnerable to cross-site scripting (XSS) via the Alert Heatmap report and the “My Reports” listing of the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2011-10038	Nagios XI versions prior to 2011R1.9 are vulnerable to cross-site scripting (XSS) via the recurring downtime script of the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2011-10037	Nagios XI versions prior to 2011R1.9 are vulnerable to cross-site scripting (XSS) via the handling of xiwindow variables used to build permalinks in the web interface. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2011-10035	Nagios XI versions prior to 2011R1.9 contain privilege escalation vulnerabilities in the scripts that install or update system crontab entries. Due to time-of-check/time-of-use race conditions and missing synchronization or final-path validation, a local low-privileged user could manipulate filesystem state during crontab installation to influence the files or commands executed with elevated privileges, resulting in execution with higher privileges.	N/A	More Details
CVE-2025-12516	Lack of Graceful Error Handling - HTTP 5xx ErrorThis issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-8850	In danny-avila/librechat version 0.7.9, there is an insecure API design issue in the 2-Factor Authentication (2FA) flow. The system allows users to disable 2FA without requiring a valid OTP or backup code, bypassing the intended verification process. This vulnerability occurs because the backend does not properly validate the OTP or backup code when the API endpoint '/api/auth/2fa/disable' is directly accessed. This flaw can be exploited by authenticated users to weaken the security of their own accounts, although it does not lead to full account compromise.	N/A	More Details
CVE-2025-62265	Cross-site scripting (XSS) vulnerability in the Blogs widget in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, 7.3 GA through update 36, and older unsupported versions allows remote attackers to inject arbitrary web script or HTML via a crafted <iframe> injected into a blog entry's “Content” text field The Blogs widget in Liferay DXP does not add the sandbox attribute to <iframe> elements, which allows remote attackers to access the parent page via scripts and links in the frame page.	N/A	More Details
CVE-2025-64118	node-tar is a Tar for Node.js. In 7.5.1, using .t (aka .list) with { sync: true } to read tar entry contents returns uninitialized memory contents if tar file was changed on disk to a smaller size while being read. This vulnerability is fixed in 7.5.2.	N/A	More Details
CVE-2025-64116	Movary is a web application to track, rate and explore your movie watch history. Prior to 0.69.0, the login page accepts a redirect parameter without validation, allowing attackers to redirect authenticated users to arbitrary external sites. This vulnerability is fixed in 0.69.0.	N/A	More Details
CVE-2025-64115	Movary is a web application to track, rate and explore your movie watch history. Versions up to and including 0.68.0 use the HTTP Referer header value directly for redirects in multiple settings endpoints, allowing a crafted link to cause an open redirect to an attacker-controlled site and facilitate phishing. This vulnerability is fixed in 0.69.0.	N/A	More Details
CVE-2025-62266	By default, Liferay Portal 7.4.0 through 7.4.3.119, and older unsupported versions, and Liferay DXP 2024.Q1.1 through 2024.Q1.5, 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions is vulnerable to DNS rebinding attacks, which allows remote attackers to redirect users to arbitrary external URLs. This vulnerability can be mitigated by changing the redirect URL security from IP to domain.	N/A	More Details

CVE-2025-64096	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prier to 1.4.2, there is a missing bounds check in Crypto_Key_update() (crypto_key_mgmt.c) which allows a remote attacker to trigger a stack-based buffer overflow by supplying a TLV packet with a spoofed length field. The function calculates the number of keys from an attacker-controlled field (pdu_len), which may exceed the static array size (kblk[98]), leading to an out-of-bounds write and potential memory corruption. This vulnerability is fixed in 1.4.2.	N/A	More Details
CVE-2025-12060	The keras.utils.get_file API in Keras, when used with the extract=True option for tar archives, is vulnerable to a path traversal attack. The utility uses Python's tarfile.extractall function without the filter="data" feature. A remote attacker can craft a malicious tar archive containing special symlinks, which, when extracted, allows them to write arbitrary files to any location on the filesystem outside of the intended destination folder. This vulnerability is linked to the underlying Python tarfile weakness, identified as CVE-2025-4517. Note that upgrading Python to one of the versions that fix CVE-2025-4517 (e.g. Python 3.13.4) is not enough. One additionally needs to upgrade Keras to a version with the fix (Keras 3.12).	N/A	More Details
CVE-2025-62257	Password enumeration vulnerability in Liferay Portal 7.4.0 through 7.4.3.119, and older unsupported versions, and Liferay DXP 2024.Q1.1 through 2024.Q1.5, 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows remote attackers to determine a user’s password even if account lockout is enabled via brute force attack.	N/A	More Details
CVE-2025-12517	Credits Page not Matching Versions in Use in the FirmwareThis issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2023-7322	Nagios Log Server versions prior to 2024R1 contain an incorrect authorization vulnerability. Users who lacked the required API permission were nevertheless able to invoke API endpoints, resulting in unintended access to data and actions exposed via the API. This incorrect authorization check could allow authenticated but non-privileged users to read or modify resources beyond their intended rights.	N/A	More Details
CVE-2023-7323	Nagios Log Server versions prior to 2024R1 are vulnerable to cross-site scripting (XSS) via the Create User function. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2023-7325	Anheng Mingyu Operation and Maintenance Audit and Risk Control System up to 2023-08-10 contains a server-side request forgery (SSRF) vulnerability in the xmlrpc.sock handler. The product accepts specially crafted XML-RPC requests that can be used to instruct the server to connect to internal unix socket RPC endpoints and perform privileged XML-RPC methods. An attacker able to send such requests can invoke administrative RPC methods via the unix socket interface to create arbitrary user accounts on the system, resulting in account creation and potential takeover of the bastion host. VulnCheck has observed this vulnerability being exploited in the wild as of 2025-10-30 at 00:30:17.837319 UTC.	N/A	More Details
CVE-2025-12554	Missing Security Headers.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-62267	Multiple cross-site scripting (XSS) vulnerabilities in web content template’s select structure page in Liferay Portal 7.4.3.35 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 update 35 through update 92 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user’s (1) First Name, (2) Middle Name, or (3) Last Name text field.	N/A	More Details
CVE-2025-62264	Reflected cross-site scripting (XSS) vulnerability in Languauge Override in Liferay Portal 7.4.3.8 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, and 7.4 update 4 through update 92 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_portal_language_override_web_internal_portlet_PLOPortlet_selectedLanguageId` parameter.	N/A	More Details
CVE-2025-6075	If the value passed to os.path.expandvars() is user-controlled a performance degradation is possible when expanding environment variables.	N/A	More Details
CVE-2025-35980	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2025. Notes: none.	N/A	More Details
CVE-2025-62797	FluxCP is a web-based Control Panel for rAthena servers written in PHP. A critical Cross-Site Request Forgery (CSRF) vulnerability exists in the FluxCP-based website template used by multiple rAthena/Ragnarok servers. State-changing POST endpoints accept browser-initiated requests that are authorized solely by the session cookie without per-request anti-CSRF tokens or robust Origin/Referer validation. An attacker who can lure a logged-in user to an attacker-controlled page can cause that user to perform sensitive actions without their intent. This vulnerability is fixed with commit e3f130c.	N/A	More Details
	D-Link DNS-343 ShareCenter devices running firmware versions up to and including 1.05 contain a command		

CVE-2018-25120	injection vulnerability in the Mail Test functionality. The web maintenance script posts to the internal goForm endpoint '/goform/Mail_Test' and uses several form parameters directly in a call to a system email utility without proper input validation. An unauthenticated remote attacker can supply crafted form data that injects shell commands, resulting in execution as root on the device. NOTE: The DNS-343 product line has been declared end-of-life.	N/A	More Details
CVE-2025-10920	GIMP ICNS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ICNS files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27684.	N/A	More Details
CVE-2025-10921	GIMP HDR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of HDR files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27803.	N/A	More Details
CVE-2025-10922	GIMP DCM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27863.	N/A	More Details
CVE-2025-10923	GIMP WBMP File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WBMP files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27878.	N/A	More Details
CVE-2025-12553	Email Server Certificate Verification Disabled.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-62276	The Document Library and the Adaptive Media modules in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions uses an incorrect cache-control header, which allows local users to obtain access to downloaded files via the browser's cache.	N/A	More Details
CVE-2025-12552	Insufficient Password Policy.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-10924	GIMP FF File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of FF files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27836.	N/A	More Details
CVE-2025-10925	GIMP ILBM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ILBM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27793.	N/A	More Details
CVE-2025-10934	GIMP XWD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XWD files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27823.	N/A	More Details
CVE-2025-	win-cli-mcp-server resolveCommandPath Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of win-cli-mcp-server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the resolveCommandPath method. The issue results from the lack of proper validation of a user-supplied	N/A	More Details

11202	string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-27787.		
CVE-2025-64389	The web server of the device performs exchanges of sensitive information in clear text through an insecure protocol.	N/A	More Details
CVE-2025-64388	Denial of service of the web server through specific requests to this protocol	N/A	More Details
CVE-2025-64387	The web application is vulnerable to a so-called ‘clickjacking’ attack. In this type of attack, the vulnerable page is inserted into a page controlled by the attacker in order to deceive the victim. This deception can range from making the victim click on a button to making them enter their login credentials in a form that, a priori, appears legitimate.	N/A	More Details
CVE-2025-64385	The equipment initially can be configured using the manufacturer's application, by Wi-Fi, by the web server or with the manufacturer’s software. Using the manufacturer's software, the device can be configured via UDP. Analyzing this communication, it has been observed that any aspect of the initial configuration can be changed by means of the device's MAC without the need for authentication.	N/A	More Details
CVE-2025-11203	LiteLLM Information health API_KEY Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of LiteLLM. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of the API_KEY parameter provided to the health endpoint. The issue results from exposing sensitive information to an unauthorized actor. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-26585.	N/A	More Details
CVE-2025-10693	When SmartStart Inclusion fails during the onboarding of a Z-Wave PIR sensor, the sensor will join the network as a non-secure device. This vulnerability exists in Silicon Labs' Z-Wave PIR Sensor Reference design delivered as part of SiSDK v2025.6.0 and v2025.6.1.	N/A	More Details
CVE-2025-62275	Blogs in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions does not check permission of images in a blog entry, which allows remote attackers to view the images in a blog entry via crafted URL.	N/A	More Details
CVE-2024-13993	Nagios XI versions prior to < 2024R1.1.2 are vulnerable to a reflected cross-site scripting (XSS) via the login page when accessed with older web browsers. Insufficient validation or escaping of user-supplied input reflected by the login page can allow an attacker to craft a malicious link that, when visited by a victim, executes arbitrary JavaScript in the victim’s browser within the Nagios XI origin. The issue is observable under legacy browser behaviors; modern browsers may mitigate some vectors.	N/A	More Details
CVE-2025-40107	In the Linux kernel, the following vulnerability has been resolved: can: hi311x: fix null pointer dereference when resuming from sleep before interface was enabled This issue is similar to the vulnerability in the `mcp251x` driver, which was fixed in commit 03c427147b2d ("can: mcp251x: fix resume from sleep before interface was brought up"). In the `hi311x` driver, when the device resumes from sleep, the driver schedules `priv->restart_work`. However, if the network interface was not previously enabled, the `priv->wq` (workqueue) is not allocated and initialized, leading to a null pointer dereference. To fix this, we move the allocation and initialization of the workqueue from the `hi3110_open` function to the `hi3110_can_probe` function. This ensures that the workqueue is properly initialized before it is used during device resume. And added logic to destroy the workqueue in the error handling paths of `hi3110_can_probe` and in the `hi3110_can_remove` function to prevent resource leaks.	N/A	More Details
CVE-2024-13998	Nagios XI versions prior to 2024R1.1.3, under certain circumstances, disclose sensitive user account information (including API keys and hashed passwords) to authenticated users who should not have access to that data. Exposure of API keys or password hashes could lead to account compromise, abuse of API privileges, or offline cracking attempts. CVE-2024-13995 addresses a similar vulnerability with a potentially incomplete fix for the underlying problem in earlier versions.	N/A	More Details
CVE-2024-13997	Nagios XI versions prior to 2024R1.1.3 contain a privilege escalation vulnerability in which an authenticated administrator could leverage the Migrate Server feature to obtain root privileges on the underlying XI host. By abusing the migration workflow, an admin-level attacker could execute actions outside the intended security scope of the application, resulting in full control of the operating system.	N/A	More Details
CVE-2021-47698	Nagios XI versions prior to 5.8.7 using embedded Nagios Core are vulnerable to cross-site scripting (XSS) via the Core UI’s Views URL handling. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2016-15054	Nagios XI versions prior to 5.4.0 are vulnerable to cross-site scripting (XSS) via the jQuery Migrate library. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details

CVE-2025-63593	Grav CMS1.7.49.5 is vulnerable to Cross Site Scripting (XSS).	N/A	More Details
CVE-2025-12642	lighttpd1.4.80 incorrectly merged trailer fields into headers after http request parsing. This behavior can be exploited to conduct HTTP Header Smuggling attacks. Successful exploitation may allow an attacker to: * Bypass access control rules * Inject unsafe input into backend logic that trusts request headers * Execute HTTP Request Smuggling attacks under some conditions This issue affects lighttpd1.4.80	N/A	More Details
CVE-2025-8558	Insider Threat Management (ITM) Server versions prior to 7.17.2 contain an authentication bypass vulnerability that allows unauthenticated users on an adjacent network to perform agent unregistration when the number of registered agents exceeds the licensed limit. Successful exploitation prevents the server from receiving new events from affected agents, resulting in a partial loss of integrity and availability with no impact to confidentiality.	N/A	More Details
CVE-2025-45959	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-14012	Potential privilege escalation issue in Revenera InstallShield version 2023 R1 running a renamed Setup.exe on Windows. When a local administrator executes a renamed Setup.exe, the MPR.dll may get loaded from an insecure location and can result in a privilege escalation. The issue has been fixed in versions 2023 R2 and later.	N/A	More Details
CVE-2025-11761	A potential security vulnerability has been identified in the HP Client Management Script Library software, which might allow escalation of privilege during the installation process. HP is releasing software updates to mitigate the potential vulnerability.	N/A	More Details
CVE-2025-12147	In Search Guard FLX versions 3.1.1 and earlier, Field-Level Security (FLS) rules are improperly enforced on object-valued fields. When an FLS exclusion rule (e.g., ~field) is applied to a field which contains an object as its value, the object is correctly removed from the _source returned by search operations. However, the object members (i.e., child attributes) remain accessible to search queries. This exposure allows adversaries to infer or reconstruct the original contents of the excluded object. Workaround - If you cannot upgrade immediately and FLS exclusion rules are used for object valued attributes (like ~object), add an additional exclusion rule for the members of the object (like ~object.*).	N/A	More Details
CVE-2025-1549	A local privilege escalation vulnerability in the WatchGuard Mobile VPN with SSL client on Windows enables a local user to execute arbitrary commands with elevated privileges on the Windows system. This vulnerability is an additional unmitigated attack path for CVE-2024-4944. This vulnerability is resolved in the Mobile VPN with SSL client for Windows version 12.11.3	N/A	More Details
CVE-2025-12148	In Search Guard versions 3.1.1 and earlier, Field Masking (FM) rules are improperly enforced on fields of type IP (IP Address). While the content of these fields is properly redacted in the _source document returned by search operations, the results do return documents (hits) when searching based on a specific IP values. This allows to reconstruct the original contents of the field. Workaround - If you cannot upgrade immediately, you can avoid the problem by using field level security (FLS) protection on fields of the affected types instead of field masking.	N/A	More Details
CVE-2025-12476	Resource Lacking AuthN.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-12603	/etc/timezone can be Arbitrarily Written.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12602	/etc/avahi/services/z9.service can be Arbitrarily Written.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12601	Denial of Service Due to SlowLoris.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-12600	Web UI Malfunction when setting unexpected locale via API.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details
CVE-2025-40087	In the Linux kernel, the following vulnerability has been resolved: NFSD: Define a proc_layoutcommit for the FlexFiles layout type Avoid a crash if a pNFS client should happen to send a LAYOUTCOMMIT operation on a FlexFiles layout.	N/A	More Details

CVE-2025-12477	Server Version Disclosure.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-12478	Non-Compliant TLS Configuration.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-12479	Systemic Lack of Cross-Site Request Forgery (CSRF) Token Implementation.This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5 .	N/A	More Details
CVE-2025-11466	Allegra DatabaseBackupBL Directory Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Allegra. Authentication is required to exploit this vulnerability. The specific flaw exists within the DatabaseBackupBL class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-27136.	N/A	More Details
CVE-2025-64386	The equipment grants a JWT token for each connection in the timeline, but during an active valid session, a hijacking of the token can be done. This will allow an attacker with the token modify parameters of security, access or even steal the session without the legitimate and active session detecting it. The web server allows the attacker to reuse an old session JWT token while the legitimate session is active.	N/A	More Details
CVE-2025-12460	An XSS issue was discovered in Afterlogic Aurora webmail version 9.8.3 and below. An attacker can send a specially crafted HTML e-mail message with JavaScript in an img HTML tag. This could allow a remote attacker to load arbitrary JavaScript code in the context of a webmail user's browser window, and access user data.	N/A	More Details
CVE-2024-14008	Nagios XI versions prior to 2024R1.3.2 contain a remote command execution vulnerability in the WinRM Configuration Wizard. Insufficient validation of user-supplied input allows an authenticated administrator to inject shell metacharacters that are incorporated into backend command invocations. Successful exploitation enables arbitrary command execution with the privileges of the Nagios XI web application user.	N/A	More Details
CVE-2025-34272	In Nagios Log Server versions prior to 2024R2.0.3, when a user's configured default dashboard is deleted, the application does not reliably fall back to an empty, default dashboard. In some implementations this can result in an unexpected dashboard being presented as the user's default view. Depending on the product's dashboard sharing and access policies, this behavior may cause information exposure or unexpected privilege exposure.	N/A	More Details
CVE-2025-34271	Nagios Log Server versions prior to 2024R2.0.2 contain a vulnerability in the cluster manager component when requesting sensitive credentials from peer nodes over an unencrypted channel even when SSL/TLS is enabled in the product configuration. As a result, an attacker positioned on the network path can intercept credentials in transit. Captured credentials could allow the attacker to authenticate as a cluster node or service account, enabling further unauthorized access, lateral movement, or system compromise.	N/A	More Details
CVE-2025-34270	Nagios Log Server versions prior to 2024R2.0.2 contain a vulnerability in the AD/LDAP user import functionality as it fails to obfuscate the password field during import. As a result, the plaintext password supplied for imported accounts may be exposed in the user interface, logs, or other diagnostic output. This can leak sensitive credentials to administrators or anyone with access to import results.	N/A	More Details
CVE-2025-34269	Nagios Fusion versions prior to R2.1 contain a vulnerability due to the application not requiring re-authentication or session rotation when a user has enabled two-factor authentication (2FA). As a result, an adversary who has obtained a valid session could continue using the active session after the target user enabled 2FA, potentially preventing the legitimate user from locking the attacker out and enabling persistent account takeover.	N/A	More Details
CVE-2025-34249	Nagios Fusion versions prior to 2024R2.1 contain a brute-force bypass in the Two-Factor Authentication (2FA) implementation. The application did not properly enforce rate limiting or account lockout for repeated failed 2FA verification attempts, allowing a remote attacker to repeatedly try second-factor codes for a targeted account. By abusing the lack of enforcement, an attacker could eventually successfully authenticate to accounts protected by 2FA.	N/A	More Details
CVE-2025-34135	Nagios XI versions prior to 2024R1.4.2 configure some systemd unit files with permission sets that were too permissive. In particular, the nagios.service unit had executable permissions that were not required. Overly permissive permissions on service unit files can broaden local attack surface by enabling unintended execution behaviors or facilitating abuse of service operations when combined with other weaknesses.	N/A	More Details
CVE-2025-	Nagios XI versions prior to 2024R1.4.2 contain a remote code execution vulnerability in the Business Process Intelligence (BPI) component. Insufficient validation and sanitization of administrator-controlled BPI configuration parameters (notably bpi_logfile and bpi_configfile) allow an authenticated administrative user to cause the product to create or overwrite files within the webroot and subsequently edit them via the BPI configuration editor. When such files carry executable extensions and are served by the web application,	N/A	More Details

34134	arbitrary code may be executed in the context of the web application user. Successful exploitation results in arbitrary command execution with the privileges of the Nagios XI web application user and can be leveraged to gain further control of the underlying host operating system.		
CVE-2024-58273	Nagios Log Server versions prior to 2024R1.0.2 contain a local privilege escalation vulnerability that allows an attacker who could execute commands as the Apache web user (or the backend shell user) to escalate to root on the host.	N/A	More Details
CVE-2024-58272	Nagios Log Server versions prior to 2024R1 contain a stored cross-site scripting (XSS) vulnerability where an attacker-supplied username containing JavaScript is stored and later rendered without proper encoding/escaping in admin or user-facing pages. When an authenticated victim loads the affected page, the browser executes the injected script in the victim's context.	N/A	More Details
CVE-2024-14009	Nagios XI versions prior to 2024R1.0.1 contain a privilege escalation vulnerability in the System Profile component. The System Profile feature is an administrative diagnostic/configuration capability. Due to improper access controls and unsafe handling of exported/imported profile data and operations, an authenticated administrator could exploit this vulnerability to execute actions on the underlying XI host outside the application's security scope. Successful exploitation may allow an administrator to obtain root privileges on the XI server.	N/A	More Details
CVE-2024-14006	Nagios XI versions prior to 2024R1.2.2 contain a host header injection vulnerability. The application trusts the user-supplied HTTP Host header when constructing absolute URLs without sufficient validation. An unauthenticated, remote attacker can supply a crafted Host header to poison generated links or responses, which may facilitate phishing of credentials, account recovery link hijacking, and web cache poisoning.	N/A	More Details
CVE-2025-4952	Tampering of the registry entries might have led to preventing the ESET security products from starting correctly on the next system startup or to unauthorized changes in the product's configuration.	N/A	More Details
CVE-2024-14005	Nagios XI versions prior to 2024R1.2 contain a command injection vulnerability in the Docker Wizard. Insufficient validation of user-supplied input in the wizard allows an authenticated administrator to inject shell metacharacters that are incorporated into backend command invocations. Successful exploitation enables arbitrary command execution with the privileges of the Nagios XI web application user.	N/A	More Details
CVE-2024-14004	Nagios XI versions prior to 2024R1.2 contain a privilege escalation vulnerability related to NagVis configuration handling (nagvis.conf). An authenticated user could manipulate NagVis configuration data or leverage insufficiently validated configuration settings to obtain elevated privileges on the Nagios XI system.	N/A	More Details
CVE-2024-14003	Nagios XI versions prior to 2024R1.2 are vulnerable to remote code execution (RCE) through its NRDP (Nagios Remote Data Processor) server plugins. Insufficient validation of inbound NRDP request parameters allows crafted input to reach command execution paths, enabling attackers to execute arbitrary commands on the underlying host in the context of the web/Nagios service.	N/A	More Details
CVE-2024-14002	Nagios XI versions prior to 2024R1.1.4 contain a local file inclusion (LFI) vulnerability via its NagVis integration. An authenticated user can supply crafted path values that cause the server to include local files, potentially exposing sensitive information from the underlying host.	N/A	More Details
CVE-2024-14001	Nagios XI versions prior to 2024R1.1.3 are vulnerable to cross-site scripting (XSS) via the Executive Summary Report component. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2024-14000	Nagios XI versions prior to 2024R1.1.3 are vulnerable to cross-site scripting (XSS) via the Capacity Planning Report component. Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2024-13999	Nagios XI versions prior to 2024R1.1.3, under certain circumstances, disclose the server's Active Directory (AD) or LDAP authentication token to an authenticated user. Exposure of the server’s AD/LDAP token could allow domain-wide authentication misuse, escalation of privileges, or further compromise of network-integrated systems.	N/A	More Details
CVE-2024-13996	Nagios XI versions prior to 2024R1.1.3 did not invalidate all other active sessions for a user when that user's password was changed. As a result, any pre-existing sessions (including those potentially controlled by an attacker) remained valid after a credential update. This insufficient session expiration could allow continued unauthorized access to user data and actions even after a password change.	N/A	More Details
CVE-2024-13995	Nagios XI versions prior to 2024R1.1.2 may (confirmed in 2024R1.1 and 2024R1.1.1) disclose sensitive user account information (including API keys and hashed passwords) to authenticated users who should not have access to that data. Exposure of API keys or password hashes could lead to account compromise, abuse of API privileges, or offline cracking attempts.	N/A	More Details
CVE-2024-	Nagios XI versions prior to 2024R1.1.2 contain a missing authorization control when the 'Allow Insecure Logins' option is enabled. Under this configuration, any user can create valid login credentials for other users without proper authorization. This can lead to unauthorized account creation, privilege escalation, or full	N/A	More Details

13994	compromise of the Nagios XI web interface depending on the target account.		
CVE-2025-34273	Nagios Log Server versions prior to 2024R2.0.3 contain an incorrect authorization vulnerability that allows non-administrator users to delete global dashboards. The application did not correctly enforce authorization checks for the global dashboard deletion workflow, enabling lower-privileged users to remove dashboards that affect other users or the overall monitoring UI.	N/A	More Details
CVE-2025-34274	Nagios Log Server versions prior to 2024R2.0.3 contain an execution with unnecessary privileges vulnerability as it runs its embedded Logstash process as the root user. If an attacker is able to compromise the Logstash process - for example by exploiting an insecure plugin, pipeline configuration injection, or a vulnerability in input parsing - the attacker could execute code with root privileges, resulting in full system compromise. The Logstash service has been altered to run as the lower-privileged 'nagios' user to reduce this risk associated with a network-facing service that can accept untrusted input or load third-party components.	N/A	More Details
CVE-2025-34277	Nagios Log Server versions prior to 2024R1.3.1 contain a code injection vulnerability where malformed dashboard ID values are not properly validated before being forwarded to an internal API. An attacker able to supply crafted dashboard ID values can cause the system to execute attacker-controlled data, leading to arbitrary code execution in the context of the Log Server process.	N/A	More Details
CVE-2025-34278	Nagios Network Analyzer versions prior to 2024R1 contain a stored cross-site scripting (XSS) vulnerability in the Source Groups page (percentile calculator menu). An attacker can supply a malicious payload which is stored by the application and later rendered in the context of other users. When a victim views the affected page the injected script executes in the victim's browser context.	N/A	More Details
CVE-2025-9869	Razer Synapse 3 Macro Module Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Razer Synapse 3. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Razer Synapse Service. By creating a symbolic link, an attacker can abuse the service to delete arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-26374.	N/A	More Details
CVE-2024-13992	Nagios XI versions prior to < 2024R1.1 is vulnerable to a cross-site scripting (XSS) when a user visits the "missing page" (404) page after following a link from another website. The vulnerable component, page-missing.php, fails to properly validate or escape user-supplied input, allowing an attacker to craft a malicious link that, when visited by a victim, executes arbitrary JavaScript in the victim’s browser within the Nagios XI domain.	N/A	More Details
CVE-2025-9870	Razer Synapse 3 RazerPhilipsHueUninstall Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Razer Synapse 3. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Philips HUE module installer. By creating a symbolic link, an attacker can abuse the installer to delete arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-26375.	N/A	More Details
CVE-2025-9871	Razer Synapse 3 Chroma Connect Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Razer Synapse 3. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Razer Chroma SDK installer. By creating a symbolic link, an attacker can abuse the installer to delete arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-26373.	N/A	More Details
CVE-2025-64158	Rejected reason: Not used	N/A	More Details
CVE-2025-11428	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11602	Potential information leak in bolt protocol handshake in Neo4j Enterprise and Community editions allows attacker to obtain one byte of information from previous connections. The attacker has no control over the information leaked in server responses.	N/A	More Details
CVE-2025-40106	In the Linux kernel, the following vulnerability has been resolved: comedi: fix divide-by-zero in comedi_buf_munge() The comedi_buf_munge() function performs a modulo operation `async->munge_chan %= async->cmd.chanlist_len` without first checking if chanlist_len is zero. If a user program submits a command with chanlist_len set to zero, this causes a divide-by-zero error when the device processes data in the interrupt handler path. Add a check for zero chanlist_len at the beginning of the function, similar to the existing checks for !map and CMDF_RAWDATA flag. When chanlist_len is zero, update munge_count and return early, indicating the data was handled without munging. This prevents potential kernel panics from malformed user commands.	N/A	More Details

CVE-2025-11843	Therefore Corporation GmbH has recently become aware that Therefore™ Online and Therefore™ On-Premises contain an account impersonation vulnerability. A malicious user may potentially be able to impersonate the web service account or the account of a service using the API when connecting to the Therefore™ Server. If the malicious user gains this impersonation user access, then it is possible for them to access the documents stored in Therefore™. This impersonation is at application level (Therefore access level), not the operating system level.	N/A	More Details
CVE-2025-8849	LibreChat version 0.7.9 is vulnerable to a Denial of Service (DoS) attack due to unbounded parameter values in the `/api/memories` endpoint. The `key` and `value` parameters accept arbitrarily large inputs without proper validation, leading to a null pointer error in the Rust-based backend when excessively large values are submitted. This results in the inability to create new memories, impacting the stability of the service.	N/A	More Details
CVE-2025-6176	Scrapy versions up to 2.13.2 are vulnerable to a denial of service (DoS) attack due to a flaw in its brotli decompression implementation. The protection mechanism against decompression bombs fails to mitigate the brotli variant, allowing remote servers to crash clients with less than 80GB of available memory. This occurs because brotli can achieve extremely high compression ratios for zero-filled data, leading to excessive memory consumption during decompression.	N/A	More Details
CVE-2025-52664	SQL injection in Revive Adserver 6.0.0 causes potential disruption or information access when specifically crafted payloads are sent by logged in users	N/A	More Details
CVE-2025-48982	This vulnerability in Veeam Agent for Microsoft Windows allows for Local Privilege Escalation if a system administrator is tricked into restoring a malicious file.	N/A	More Details
CVE-2025-48980	In Brave Browser Desktop versions prior to 1.83.10 that have the split view feature enabled, the "Open Link in Split View" context menu item did not respect the SameSite cookie attribute. Therefore SameSite=Strict cookies would be sent on a cross-site navigation using this method.	N/A	More Details
CVE-2025-27208	A reflected Cross-Site Scripting (XSS) vulnerability has been identified in Revive Adserver version 5.5.2. An attacker could trick a user with access to the user interface of a Revive Adserver instance into clicking on a specifically crafted URL and execute injected JavaScript code in the context of the victim's browser. The session cookie cannot be accessed, but a number of other operations could be performed. The vulnerability is present in the admin-search.php file and can be exploited via the compact parameter.	N/A	More Details
CVE-2025-34298	Nagios Log Server versions prior to 2024R1.3.2 contain a privilege escalation vulnerability in the account email-change workflow. A user could set their own email to an invalid value and, due to insufficient validation and authorization checks tied to email identity state, trigger inconsistent account state that granted elevated privileges or bypassed intended access controls.	N/A	More Details
CVE-2025-34287	Nagios XI versions prior to 2024R2 contain an improperly owned script, process_perfdata.pl, which is executed periodically as the nagios user but owned by www-data. Because the file was writable by www-data, an attacker with web server privileges could modify its contents, leading to arbitrary code execution as the nagios user when the script is next run. This improper ownership and permission configuration enables local privilege escalation.	N/A	More Details
CVE-2025-34286	Nagios XI versions prior to 2026R1 contain a remote code execution vulnerability in the Core Config Manager (CCM) Run Check command. Insufficient validation/escaping of parameters used to build backend command lines allows an authenticated administrator to inject shell metacharacters that are executed on the server. Successful exploitation results in arbitrary command execution with the privileges of the Nagios XI web application user and can be leveraged to gain control of the underlying host operating system.	N/A	More Details
CVE-2025-34284	Nagios XI versions prior to 2024R2 contain a command injection vulnerability in the WinRM plugin. Insufficient validation of user-supplied parameters allows an authenticated administrator to inject shell metacharacters that are incorporated into backend command invocations. Successful exploitation enables arbitrary command execution with the privileges of the Nagios XI web application user and can be leveraged to modify configuration, exfiltrate data, disrupt monitoring operations, or execute commands on the underlying host operating system.	N/A	More Details
CVE-2025-34283	Nagios XI versions prior to 2024R1.4.2 revealed API keys to users who were not authorized for API access when using Neptune themes. An authenticated user without API privileges could view another user's or their own API key value.	N/A	More Details
CVE-2025-34280	Nagios Network Analyzer versions prior to 2024R2.0.1 contain a vulnerability in the LDAP certificate management functionality whereby the certificate removal operation fails to apply adequate input sanitation. An authenticated administrator can trigger command execution on the underlying host in the context of the web application service, resulting in remote code execution with the service's privileges.	N/A	More Details
CVE-2025-12599	Multiple Devices are Sharing the Same Secrets for SDKSocket (TCP/5000).This issue affects BLU-IC2: through 1.19.5; BLU-IC4: through 1.19.5.	N/A	More Details