SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 September 2025

Generated on 03 September 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-2025-49387	Unrestricted Upload of File with Dangerous Type vulnerability in add-ons.org Drag and Drop File Upload for Elementor Forms allows Upload a Web Shell to a Web Server. This issue affects Drag and Drop File Upload for Elementor Forms: from n/a through 1.5.3.	10.0	More Details
CVE-2025-58048	Paymenter is a free and open-source webshop solution for hostings. Prior to version 1.2.11, the ticket attachments functionality in Paymenter allows a malicious authenticated user to upload arbitrary files. This could result in sensitive data extraction from the database, credentials being read from configuration files, and arbitrary system commands being run under the web server user context. This vulnerability was patched by commit 87c3db4 and was released under the version 1.2.11 tag without any other code modifications compared to version 1.2.10. If upgrading is not immediately possible, administrators can mitigate this vulnerability with one or more of the following measures: updating nginx config to download attachments	9.9	More Details

	instead of executing them or disallowing access to /storage/ fully using a WAF such as Cloudflare.		
CVE-2025-9523	A vulnerability was detected in Tenda AC1206 15.03.06.23. Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2025-54725	Authentication Bypass Using an Alternate Path or Channel vulnerability in uxper Golo allows Authentication Abuse. This issue affects Golo: from n/a through 1.7.0.	9.8	More Details
CVE-2025-8857	Clinic Image System developed by Changing contains hard-coded Credentials, allowing unauthenticated remote attackers to log into the system using administrator credentials embedded in the source code.	9.8	More Details
CVE-2025-9605	A security vulnerability has been detected in Tenda AC21 and AC23 16.03.08.16. Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. Such manipulation of the argument mac leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2025-55583	D-Link DIR-868L B1 router firmware version FW2.05WWB02 contains an unauthenticated OS command injection vulnerability in the fileaccess.cgi component. The endpoint /dws/api/UploadFile accepts a pre_api_arg parameter that is passed directly to system-level shell execution functions without sanitization or authentication. Remote attackers can exploit this to execute arbitrary commands as root via crafted HTTP requests.	9.8	More Details
CVE-2025-54738	Authentication Bypass Using an Alternate Path or Channel vulnerability in NooTheme Jobmonster allows Authentication Abuse. This issue affects Jobmonster: from n/a through 4.7.9.	9.8	More Details
CVE-2025-52761	Deserialization of Untrusted Data vulnerability in manfcarlo WP Funnel Manager allows Object Injection. This issue affects WP Funnel Manager: from n/a through 1.4.0.	9.8	More Details
CVE-2025-49388	Incorrect Privilege Assignment vulnerability in kamleshyadav Miraculous Core Plugin allows Privilege Escalation. This issue affects Miraculous Core Plugin: from n/a through 2.0.7.	9.8	More Details
CVE-2025-7955	The RingCentral Communications plugin for WordPress is vulnerable to Authentication Bypass due to improper validation within the ringcentral_admin_login_2fa_verify() function in versions 1.5 to 1.6.8. This makes it possible for unauthenticated attackers to log in as any user simply by supplying identical bogus codes.	9.8	More Details
CVE-2025-52122	Freeform 5.0.0 to before 5.10.16, a plugin for CraftCMS, contains an Server-side template injection (SSTI) vulnerability, resulting in arbitrary code injection for all users that have access to editing a form (submission title).	9.8	More Details

CVE-2025-50972	SQL Injection vulnerability in AbanteCart 1.4.2, allows unauthenticated attackers to execute arbitrary SQL commands via the tmpl_id parameter to index.php. Three techniques have been demonstrated: error-based injection using a crafted FLOOR-based payload, time-based blind injection via SLEEP(), and UNION-based injection to extract arbitrary data.	9.8	More Details
CVE-2025-8861	TSA developed by Changing has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents.	9.8	More Details
CVE-2025-43728	Dell ThinOS 10, versions prior to 2508_10.0127, contain a Protection Mechanism Failure vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	9.6	More Details
CVE-2025-54720	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SteelThemes Nest Addons allows SQL Injection. This issue affects Nest Addons: from n/a through 1.6.3.	9.3	More Details
CVE-2025-39496	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WBW WooBeWoo Product Filter Pro allows SQL Injection.This issue affects WooBeWoo Product Filter Pro: from n/a before 2.9.6.	9.3	More Details
CVE-2025-48100	Improper Control of Generation of Code ('Code Injection') vulnerability in extremeidea bidorbuy Store Integrator allows Remote Code Inclusion. This issue affects bidorbuy Store Integrator: from n/a through 2.12.0.	9.1	More Details
CVE-2025-58059	Valtimo is a platform for Business Process Automation. In versions before 12.16.0.RELEASE, and from 13.0.0.RELEASE to before 13.1.2.RELEASE, any admin that can create or modify and execute process-definitions could gain access to sensitive data or resources. This includes but is not limited to: running executables on the application host, inspecting and extracting data from the host environment or application properties, spring beans (application context, database pooling). The following conditions have to be met in order to perform this attack: the user must be logged in, have the admin role, and must have some knowledge about running scripts via a the Camunda/Operator engine. Version 12.16.0 and 13.1.2 have been patched. It is strongly advised to upgrade. If no scripting is needed in any of the processes, it could be possible to disable it altogether via the ProcessEngineConfiguration. However, this workaround could lead to unexpected side-effects.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
	The Video Share VOD – Turnkey Video Site Builder Script plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up		

CVE-2025-7812	to, and including, 2.7.6. This is due to missing or incorrect nonce validation on the adminExport() function. This makes it possible for unauthenticated attackers to update settings and execute remote code when the Server command execution setting is enabled via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2025-54742	Deserialization of Untrusted Data vulnerability in magepeopleteam WpEvently allows Object Injection. This issue affects WpEvently: from n/a through 4.4.8.	8.8	More Details
CVE-2025-9525	A flaw has been found in Linksys E1700 1.0.0.4.003. Affected by this vulnerability is the function setWan of the file /goform/setWan. This manipulation of the argument DeviceName/lanIp causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9526	A vulnerability has been found in Linksys E1700 1.0.0.4.003. Affected by this issue is the function setSysAdm of the file /goform/setSysAdm. Such manipulation of the argument rm_port leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-37777	O2OA v9.0.3 was discovered to contain a remote code execution (RCE) vulnerability via the mainOutput() function.	8.8	More Details
CVE-2025-9527	A vulnerability was found in Linksys E1700 1.0.0.4.003. This affects the function QoSSetup of the file /goform/QoSSetup. Performing manipulation of the argument ack_policy results in stack-based buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-50989	OPNsense 25.1 contains an authenticated command injection vulnerability in its Bridge Interface Edit endpoint (interfaces_bridge_edit.php). The span POST parameter is concatenated into a system-level command without proper sanitization or escaping, allowing an administrator to inject arbitrary shell operators and payloads. Successful exploitation grants RCE with the privileges of the web service (typically root), potentially leading to full system compromise or lateral movement. This vulnerability arises from inadequate input validation and improper handling of user-supplied data in backend command invocations.	8.8	More Details
CVE-2025-55422	In FoxCMS 1.2.6, there is a reflected Cross Site Scripting (XSS) vulnerability in /index.php/plus.	8.8	More Details
CVE-2025-	NodeBB v4.3.0 is vulnerable to SQL injection in its search-categories API endpoint (/api/v3/search/categories). The search query parameter is not	8.6	More

50979	properly sanitized, allowing unauthenticated, remote attackers to inject boolean-based blind and PostgreSQL error-based payloads.		Details
CVE-2025-39247	There is an Access Control Vulnerability in some HikCentral Professional versions. This could allow an unauthenticated user to obtain the admin permission.	8.6	More Details
CVE-2025-49404	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in purethemes Listeo-Core allows SQL Injection. This issue affects Listeo-Core: from n/a through 1.9.32.	8.5	More Details
CVE-2025-8067	A flaw was found in the Udisks daemon, where it allows unprivileged users to create loop devices using the D-BUS system. This is achieved via the loop device handler, which handles requests sent through the D-BUS interface. As two of the parameters of this handle, it receives the file descriptor list and index specifying the file where the loop device should be backed. The function itself validates the index value to ensure it isn't bigger than the maximum value allowed. However, it fails to validate the lower bound, allowing the index parameter to be a negative value. Under these circumstances, an attacker can cause the UDisks daemon to crash or perform a local privilege escalation by gaining access to files owned by privileged users.	8.5	More Details
CVE-2025-43730	Dell ThinOS 10, versions prior to 2508_10.0127, contains an Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability. A local unauthenticated user could potentially exploit this vulnerability leading to Elevation of Privileges and Information disclosure.	8.4	More Details
CVE-2025-50983	SQL Injection vulnerability exists in the sortKey parameter of the GET /api/v1/wanted/cutoff API endpoint in readarr 0.4.15.2787. The endpoint fails to properly sanitize user-supplied input, allowing attackers to inject and execute arbitrary SQL commands against the backend SQLite database. Sqlmap confirmed exploitation via stacked queries, demonstrating that the parameter can be abused to run arbitrary SQL statements. A heavy query was executed using SQLite's RANDOMBLOB() and HEX() functions to simulate a time-based payload, indicating deep control over database interactions.	8.3	More Details
CVE-2025-53572	Deserialization of Untrusted Data vulnerability in emarket-design WP Easy Contact allows Object Injection. This issue affects WP Easy Contact: from n/a through 4.0.1.	8.1	More Details
CVE-2025-53334	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in TieLabs Jannah allows PHP Local File Inclusion. This issue affects Jannah: from n/a through 7.4.1.	8.1	More Details
CVE-2025-54731	Improper Control of Generation of Code ('Code Injection') vulnerability in emarket-design YouTube Showcase allows Object Injection. This issue affects YouTube Showcase: from n/a through 3.5.1.	8.1	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ovatheme Ireca	8.1	More

54716	allows PHP Local File Inclusion. This issue affects Ireca: from n/a through 1.8.5.		Details
CVE-2025-53584	Deserialization of Untrusted Data vulnerability in emarket-design WP Ticket Customer Service Software & Support Ticket System allows Object Injection. This issue affects WP Ticket Customer Service Software & Support Ticket System: from n/a through 6.0.2.	8.1	More Details
CVE-2025-53583	Deserialization of Untrusted Data vulnerability in emarket-design Employee Spotlight allows Object Injection. This issue affects Employee Spotlight: from n/a through 5.1.1.	8.1	More Details
CVE-2025-53578	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in gavias Kipso allows PHP Local File Inclusion. This issue affects Kipso: from n/a through 1.3.4.	8.1	More Details
CVE-2025-53216	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeUniver Glamer allows PHP Local File Inclusion. This issue affects Glamer: from n/a through 1.0.2.	8.1	More Details
CVE-2025-53227	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Unfoldwp Magazine Saga allows PHP Local File Inclusion. This issue affects Magazine Saga: from n/a through 1.2.7.	8.1	More Details
CVE-2025-53243	Deserialization of Untrusted Data vulnerability in emarket-design Employee Directory – Staff Listing & Team Directory Plugin for WordPress allows Object Injection. This issue affects Employee Directory – Staff Listing & Team Directory Plugin for WordPress: from n/a through 4.5.3.	8.1	More Details
CVE-2025-53244	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Unfoldwp Magazine Elite allows PHP Local File Inclusion. This issue affects Magazine Elite: from n/a through 1.2.4.	8.1	More Details
CVE-2025-53247	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WPInterface BlogMarks allows PHP Local File Inclusion. This issue affects BlogMarks: from n/a through 1.0.8.	8.1	More Details
CVE-2025-53248	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Unfoldwp Magazine allows PHP Local File Inclusion. This issue affects Magazine: from n/a through 1.2.2.	8.1	More Details
CVE-2025-58334	In JetBrains IDE Services before 2025.5.0.1086, 2025.4.2.2164 users without appropriate permissions could assign high-privileged role for themselves	8.1	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ovatheme Ovatheme Events allows PHP Local File Inclusion. This issue affects	8.1	More Details

53576	Ovatheme Events: from n/a through 1.2.8.		
CVE-2025-49405	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in favethemes Houzez allows PHP Local File Inclusion. This issue affects Houzez: from n/a through 4.1.1.	8.1	More Details
CVE-2025-49383	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CocoBasic Neresa allows PHP Local File Inclusion. This issue affects Neresa: from n/a through 1.3.	8.1	More Details
CVE-2024-13342	The Booster for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'add_files_to_order' function in all versions up to, and including, 7.2.4. This makes it possible for unauthenticated attackers to upload arbitrary files with double extensions on the affected site's server which may make remote code execution possible. This is only exploitable on select instances where the configuration will execute the first extension present.	8.1	More Details
CVE-2025-55177	Incomplete authorization of linked device synchronization messages in WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, and WhatsApp for Mac v2.25.21.78 could have allowed an unrelated user to trigger processing of content from an arbitrary URL on a target’s device. We assess that this vulnerability, in combination with an OS-level vulnerability on Apple platforms (CVE-2025-43300), may have been exploited in a sophisticated attack against specific targeted users.	8.0	More Details
CVE-2025-43268	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6. A malicious app may be able to gain root privileges.	7.8	More Details
CVE-2025-43187	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.7.7, macOS Ventura 13.7.7, macOS Sequoia 15.6. Running an hdiutil command may unexpectedly execute arbitrary code.	7.8	More Details
CVE-2025-43882	Dell ThinOS 10, versions prior to 2508_10.0127, contains an Unverified Ownership vulnerability. A local low-privileged attacker could potentially exploit this vulnerability leading to Unauthorized Access.	7.8	More Details
CVE-2025-43729	Dell ThinOS 10, versions prior to 2508_10.0127, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A local low-privileged attacker could potentially exploit this vulnerability leading to Elevation of Privileges and Unauthorized Access.	7.8	More Details
CVE-2025-58322	NAVER MYBOX Explorer for Windows before 3.0.8.133 allows a local attacker to escalate privileges to NT AUTHORITY\SYSTEM by invoking arbitrary DLLs due to improper privilege checks.	7.8	More Details
CVE-	NAVER MYBOX Explorer for Windows before 3.0.8.133 allows a local		More

2025-58323	attacker to escalate privileges to NT AUTHORITY\SYSTEM by executing arbitrary files due to improper privilege checks.	7.7	Details
CVE-2025-54029	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in extendons WooCommerce csv import export allows Path Traversal. This issue affects WooCommerce csv import export: from n/a through 2.0.6.	7.7	More Details
CVE-2025-53588	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Dmitry V. (CEO of "UKR Solution") UPC/EAN/GTIN Code Generator allows Path Traversal. This issue affects UPC/EAN/GTIN Code Generator: from n/a through 2.0.2.	7.7	More Details
CVE-2025-53230	Missing Authorization vulnerability in honzat Page Manager for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Page Manager for Elementor: from n/a through 2.0.5.	7.6	More Details
CVE-2025-53328	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Assaf Parag Poll, Survey & Quiz Maker Plugin by Opinion Stage allows PHP Local File Inclusion. This issue affects Poll, Survey & Quiz Maker Plugin by Opinion Stage: from n/a through 19.11.0.	7.5	More Details
CVE-2025-55763	Buffer Overflow in the URI parser of CivetWeb 1.14 through 1.16 (latest) allows a remote attacker to achieve remote code execution via a crafted HTTP request. This vulnerability is triggered during request processing and may allow an attacker to corrupt heap memory, potentially leading to denial of service or arbitrary code execution.	7.5	More Details
CVE-2025-53326	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CodeYatri Gutenify allows PHP Local File Inclusion. This issue affects Gutenify: from n/a through 1.5.6.	7.5	More Details
CVE-2024-13807	The Xagio SEO plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.1.0.5 via the backup functionality due to weak filename structure and lack of protection in the directory. This makes it possible for unauthenticated attackers to extract sensitive data from backups which can include the entire database and site's files.	7.5	More Details
CVE-2025-57215	Tenda AC10 v4.0 firmware v16.03.10.20 was discovered to contain a stack overflow via the function get_parentControl_list_Info.	7.5	More Details
CVE-2025-40779	If a DHCPv4 client sends a request with some specific options, and Kea fails to find an appropriate subnet for the client, the `kea-dhcp4` process will abort with an assertion failure. This happens only if the client request is unicast directly to Kea; broadcast messages do not cause the problem. This issue affects Kea versions 2.7.1 through 2.7.9, 3.0.0, and 3.1.0.	7.5	More Details
	GLPI, which stands for Gestionnaire Libre de Parc Informatique, is a Free		

CVE-2025-53105	Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions 10.0.0 to before 10.0.19, a connected user without administration rights can change the rules execution order. This issue has been patched in version 10.0.19.	7.5	More Details
CVE-2025-58047	Volto is a React based frontend for the Plone Content Management System. In versions from 19.0.0-alpha.1 to before 19.0.0-alpha.4, 18.0.0 to before 18.24.0, 17.0.0 to before 17.22.1, and prior to 16.34.0, an anonymous user could cause the NodeJS server part of Volto to quit with an error when visiting a specific URL. The problem has been patched in versions 16.34.0, 17.22.1, 18.24.0, and 19.0.0-alpha.4. To mitigate downtime, have setup automatically restart processes that quit with an error.	7.5	More Details
CVE-2025-6203	A malicious user may submit a specially-crafted complex payload that otherwise meets the default request size limit which results in excessive memory and CPU consumption of Vault. This may lead to a timeout in Vault’s auditing subroutine, potentially resulting in the Vault server to become unresponsive. This vulnerability, CVE-2025-6203, is fixed in Vault Community Edition 1.20.3 and Vault Enterprise 1.20.3, 1.19.9, 1.18.14, and 1.16.25.	7.5	More Details
CVE-2025-36003	IBM Security Verify Governance Identity Manager 10.0.2 could allow a remote attacker to obtain sensitive information when detailed technical error messages are returned. This information could be used in further attacks against the system.	7.5	More Details
CVE-2025-8858	Clinic Image System developed by Changing has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2025-57767	Asterisk is an open source private branch exchange and telephony toolkit. Prior to versions 20.15.2, 21.10.2, and 22.5.2, if a SIP request is received with an Authorization header that contains a realm that wasn't in a previous 401 response's WWW-Authenticate header, or an Authorization header with an incorrect realm was received without a previous 401 response being sent, the get_authorization_header() function in res_pjsip_authenticator_digest will return a NULL. This wasn't being checked before attempting to get the digest algorithm from the header which causes a SEGV. This issue has been patched in versions 20.15.2, 21.10.2, and 22.5.2. There are no workarounds.	7.5	More Details
CVE-2025-9639	The QbiCRMGateway developed by Ai3 has an Arbitrary File Reading vulnerability, allowing unauthenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2025-	A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload. This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this	7.4	More

20241	vulnerability by sending a crafted IS-IS packet to an affected device. A successful exploit could allow the attacker to cause the unexpected restart of the IS-IS process, which could cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2-adjacent to the affected device.		Details
CVE-2025-9503	A security vulnerability has been detected in Campcodes Online Loan Management System 1.0. Affected is an unknown function of the file /ajax.php?action=save_borrower. The manipulation of the argument lastname leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9511	A vulnerability was identified in itsourcecode Apartment Management System 1.0. This vulnerability affects unknown code of the file /visitor/addvisitor.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-55618	In Hyundai Navigation App STD5W.EUR.HMC.230516.afa908d, an attacker can inject HTML payloads in the profile name field in navigation app which then get rendered.	7.3	More Details
CVE-2025-9510	A security vulnerability has been detected in itsourcecode Apartment Management System 1.0. The affected element is an unknown function of the file /branch/addbranch.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9502	A weakness has been identified in Campcodes Online Loan Management System 1.0. This impacts an unknown function of the file /ajax.php?action=save_payment. Executing manipulation of the argument loan_id can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-9509	A security flaw has been discovered in itsourcecode Apartment Management System 1.0. This issue affects some unknown processing of the file /report/fair_info_all.php. Performing manipulation of the argument fid results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-9505	A flaw has been found in Campcodes Online Loan Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_loan_type. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-9508	A vulnerability was detected in itsourcecode Apartment Management System 1.0. The impacted element is an unknown function of the file /report/rented_info.php. The manipulation of the argument rsid results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details

CVE-2025-9662	A vulnerability was determined in code-projects Simple Grading System 1.0. This affects an unknown function of the file /login.php of the component Admin Panel. Executing manipulation can lead to sql injection. The attack may be performed from a remote location. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-9660	A vulnerability was found in SourceCodester Bakeshop Online Ordering System 1.0. The impacted element is an unknown function of the file /passwordrecover.php. Performing manipulation of the argument phonenumber results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-9504	A vulnerability was detected in Campcodes Online Loan Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=save_plan. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-9507	A weakness has been identified in itsourcecode Apartment Management System 1.0. Impacted is an unknown function of the file /report/visitor_info.php. Executing manipulation of the argument vid can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-9506	A vulnerability has been found in Campcodes Online Loan Management System 1.0. This affects an unknown part of the file /ajax.php?action=delete_plan. Such manipulation of the argument ID leads to sql injection. The attack may be performed from a remote location. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-9610	A vulnerability was determined in code-projects Online Event Judging System 1.0. This issue affects some unknown processing of the file /create_account.php. This manipulation of the argument fname causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. Other parameters might be affected as well.	7.3	More Details
CVE-2025-9643	A vulnerability was found in itsourcecode Apartment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /setting/utility_bill_setup.php. Performing manipulation of the argument txtGasBill results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-9596	A vulnerability was determined in itsourcecode Sports Management System 1.0. This affects an unknown function of the file /login.php. This manipulation of the argument User causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-	A vulnerability was detected in itsourcecode Apartment Management System 1.0. This affects an unknown part of the file /setting/employee_salary_setup.php. The manipulation of the argument	7.3	More Details

9601	ddlEmpName results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.		
CVE-2025-9600	A security vulnerability has been detected in itsourcecode Apartment Management System 1.0. Affected by this issue is some unknown functionality of the file /setting/member_type_setup.php. The manipulation of the argument txtMemberType leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9599	A weakness has been identified in itsourcecode Apartment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /setting/month_setup.php. Executing manipulation of the argument txtMonthName can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-9533	A vulnerability has been found in TOTOLINK T10 4.1.8cu.5241_B20210927. Affected is an unknown function of the file /formLoginAuth.htm. The manipulation of the argument authCode with the input 1 leads to improper authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-9644	A vulnerability was determined in itsourcecode Apartment Management System 1.0. Affected by this issue is some unknown functionality of the file /setting/bill_setup.php. Executing manipulation of the argument txtBillType can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-9645	A vulnerability was identified in itsourcecode Apartment Management System 1.0. This affects an unknown part of the file /t_dashboard/r_all_info.php. The manipulation of the argument mid leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-40927	CGI::Simple versions before 1.282 for Perl has a HTTP response splitting flaw This vulnerability is a confirmed HTTP response splitting flaw in CGI::Simple that allows HTTP response header injection, which can be used for reflected XSS or open redirect under certain conditions. Although some validation exists, it can be bypassed using URL-encoded values, allowing an attacker to inject untrusted content into the response via query parameters. As a result, an attacker can inject a line break (e.g. %0A) into the parameter value, causing the server to split the HTTP response and inject arbitrary headers or even an HTML/JavaScript body, leading to reflected cross-site scripting (XSS), open redirect or other attacks. The issue documented in CVE-2010-4410 https://www.cve.org/CVERecord?id=CVE-2010-4410 is related but the fix was incomplete. Impact By injecting %0A (newline) into a query string parameter, an attacker can: * Break the current HTTP header * Inject a new header or entire body * Deliver a script payload that is reflected in the server’s response That can lead to the following attacks: * reflected XSS * open redirect * cache poisoning * header manipulation	7.3	More Details

CVE-2025-9598	A security flaw has been discovered in itsourcecode Apartment Management System 1.0. Affected is an unknown function of the file /setting/year_setup.php. Performing manipulation of the argument txtXYear results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-9597	A vulnerability was identified in itsourcecode Apartment Management System 1.0. This impacts an unknown function of the file /o_dashboard/rented_all_info.php. Such manipulation of the argument uid leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-9594	A vulnerability has been found in itsourcecode Apartment Management System 1.0. The affected element is an unknown function of the file /report/complain_info.php. The manipulation of the argument vid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-9593	A flaw has been found in itsourcecode Apartment Management System 1.0. Impacted is an unknown function of the file /report/unit_status_info.php. Executing manipulation of the argument usid can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-9592	A vulnerability was detected in itsourcecode Apartment Management System 1.0. This issue affects some unknown processing of the file /report/bill_info.php. Performing manipulation of the argument vid results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	7.3	More Details
CVE-2025-9529	A weakness has been identified in Campcodes Payroll Management System 1.0. The affected element is the function include of the file /index.php. This manipulation of the argument page causes file inclusion. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-58218	Deserialization of Untrusted Data vulnerability in eniturechnology Small Package Quotes – USPS Edition allows Object Injection. This issue affects Small Package Quotes – USPS Edition: from n/a through 1.3.9.	7.2	More Details
CVE-2025-48308	Cross-Site Request Forgery (CSRF) vulnerability in nonletter Newsletter subscription optin module allows Stored XSS. This issue affects Newsletter subscription optin module: from n/a through 1.2.9.	7.1	More Details
CVE-2025-48309	Cross-Site Request Forgery (CSRF) vulnerability in web-able BetPress allows Stored XSS. This issue affects BetPress: from n/a through 1.0.1 Lite.	7.1	More Details
CVE-2025-48359	Cross-Site Request Forgery (CSRF) vulnerability in thaihavnn07 ATT YouTube Widget allows Stored XSS. This issue affects ATT YouTube Widget: from n/a through 1.0.	7.1	More Details
CVE-2025-48321	Cross-Site Request Forgery (CSRF) vulnerability in dyiosah Ultimate twitter profile widget allows Stored XSS. This issue affects Ultimate twitter profile widget: from n/a through 1.0.	7.1	More Details

CVE-2025-54724	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Golo allows Reflected XSS. This issue affects Golo: from n/a through 1.7.1.	7.1	More Details
CVE-2025-48307	Cross-Site Request Forgery (CSRF) vulnerability in kasonzhao SEO For Images allows Stored XSS. This issue affects SEO For Images: from n/a through 1.0.0.	7.1	More Details
CVE-2025-54714	Missing Authorization vulnerability in Dylan James Zephyr Project Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Zephyr Project Manager: from n/a through 3.3.201.	7.1	More Details
CVE-2025-48306	Cross-Site Request Forgery (CSRF) vulnerability in developers savyour Savyour Affiliate Partner allows Stored XSS. This issue affects Savyour Affiliate Partner: from n/a through 2.1.4.	7.1	More Details
CVE-2025-48109	Cross-Site Request Forgery (CSRF) vulnerability in Xavier Media XM-Backup allows Stored XSS. This issue affects XM-Backup: from n/a through 0.9.1.	7.1	More Details
CVE-2025-54710	Missing Authorization vulnerability in bPlugins Tiktok Feed allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Tiktok Feed: from n/a through 1.0.21.	7.1	More Details
CVE-2025-48304	Cross-Site Request Forgery (CSRF) vulnerability in Gary Illyes Google XML News Sitemap plugin allows Stored XSS. This issue affects Google XML News Sitemap plugin: from n/a through 0.02.	7.1	More Details
CVE-2025-49407	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Houzez allows Reflected XSS. This issue affects Houzez: from n/a through 4.1.1.	7.1	More Details
CVE-2025-53215	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8bitkid Yahoo! WebPlayer allows Reflected XSS. This issue affects Yahoo! WebPlayer: from n/a through 2.0.6.	7.1	More Details
CVE-2025-53579	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in captcha.eu Captcha.eu allows Reflected XSS. This issue affects Captcha.eu: from n/a through n/a.	7.1	More Details
CVE-2025-53225	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eboekhouden e-Boekhouden.nl allows Reflected XSS. This issue affects e-Boekhouden.nl: from n/a through 1.9.3.	7.1	More Details
CVE-2025-53220	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in XmasB XmasB Quotes allows Reflected XSS. This issue affects XmasB Quotes: from n/a through 1.6.1.	7.1	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jason Theme Blvd Widget Areas allows	7.1	More

53289	Reflected XSS. This issue affects Theme Blvd Widget Areas: from n/a through 1.3.0.		Details
CVE-2025-53223	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in undoIT Theme Switcher Reloaded allows Reflected XSS. This issue affects Theme Switcher Reloaded: from n/a through 1.1.	7.1	More Details
CVE-2025-48320	Cross-Site Request Forgery (CSRF) vulnerability in cuckoohello 百度分享按钮 allows Stored XSS. This issue affects 百度分享按钮: from n/a through 1.0.6.	7.1	More Details
CVE-2025-53224	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Koen Schuit NextGEN Gallery Search allows Reflected XSS. This issue affects NextGEN Gallery Search: from n/a through 2.12.	7.1	More Details
CVE-2025-48351	Cross-Site Request Forgery (CSRF) vulnerability in PluginsPoint Kento Splash Screen allows Stored XSS. This issue affects Kento Splash Screen: from n/a through 1.4.	7.1	More Details
CVE-2025-48353	Cross-Site Request Forgery (CSRF) vulnerability in dactum Clickbank WordPress Plugin (Niche Storefront) allows Stored XSS. This issue affects Clickbank WordPress Plugin (Niche Storefront): from n/a through 1.3.5.	7.1	More Details
CVE-2025-48311	Cross-Site Request Forgery (CSRF) vulnerability in OffClicks Invisible Optin allows Stored XSS. This issue affects Invisible Optin: from n/a through 1.0.	7.1	More Details
CVE-2025-48325	Cross-Site Request Forgery (CSRF) vulnerability in shmish111 WP Admin Theme allows Stored XSS. This issue affects WP Admin Theme: from n/a through 1.0.	7.1	More Details
CVE-2025-20317	A vulnerability in the Virtual Keyboard Video Monitor (vKVM) connection handling of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to redirect a user to a malicious website. This vulnerability is due to insufficient verification of vKVM endpoints. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious webpage and potentially capture user credentials. Note: The affected vKVM client is also included in Cisco UCS Manager.	7.1	More Details
CVE-2025-58217	Cross-Site Request Forgery (CSRF) vulnerability in GeroNikolov Instant Breaking News allows Stored XSS. This issue affects Instant Breaking News: from n/a through 1.0.	7.1	More Details
CVE-2025-48343	Cross-Site Request Forgery (CSRF) vulnerability in Aaron Axelsen WPMU Ldap Authentication allows Stored XSS. This issue affects WPMU Ldap Authentication: from n/a through 5.0.1.	7.1	More Details
CVE-2025-	An issue was discovered in simple-admin-core v1.2.0 thru v1.6.7. The /sys-api/role/update interface in the simple-admin-core system has a	7.0	More

51667	limited SQL injection vulnerability, which may lead to partial data leakage or disruption of normal system operations.		Details
CVE-2025-5187	A vulnerability exists in the NodeRestriction admission controller in Kubernetes clusters where node users can delete their corresponding node object by patching themselves with an OwnerReference to a cluster-scoped resource. If the OwnerReference resource does not exist or is subsequently deleted, the given node object will be deleted via garbage collection.	6.7	More Details
CVE-2025-55582	D-Link DCS-825L firmware v1.08.01 contains a vulnerability in the watchdog script `mydlink-watch-dog.sh`, which blindly respawns binaries such as `dcp` and `signalc` without verifying integrity, authenticity, or permissions. An attacker with local filesystem access (via physical access, firmware modification, or debug interfaces) can replace these binaries with malicious payloads. The script executes these binaries as root in an infinite loop, leading to persistent privilege escalation and arbitrary code execution. This issue is mitigated in v1.09.02, but the product is officially End-of-Life and unsupported.	6.6	More Details
CVE-2025-9441	The iATS Online Forms plugin for WordPress is vulnerable to time-based SQL Injection via the ‘order' parameter in all versions up to, and including, 1.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-51972	A SQL Injection vulnerability exists in the login.php of PuneethReddyHC Online Shopping System Advanced 1.0 due to improper sanitization of user-supplied input in the keyword POST parameter.	6.5	More Details
CVE-2025-20344	A vulnerability in the backup restore functionality of Cisco Nexus Dashboard could allow an authenticated, remote attacker to conduct a path traversal attack on an affected device. This vulnerability is due to insufficient validation of the contents of a backup file. An attacker with valid Administrator credentials could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to gain root privileges on the underlying shell on the affected device.	6.5	More Details
CVE-2025-20294	Multiple vulnerabilities in the CLI and web-based management interface of Cisco UCS Manager Software could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. These vulnerabilities are due to insufficient input validation of command arguments supplied by the user. An attacker could exploit these vulnerabilities by authenticating to a device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of the affected device with root-level privileges.	6.5	More Details

CVE-2025-54598	The Bevy Event service through 2025-07-22, as used for eBay Seller Events and other activities, allows CSRF to delete all notifications via the /notifications/delete/ URI.	6.5	More Details
CVE-2025-49402	Missing Authorization vulnerability in favethemes Houzez CRM allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Houzez CRM: from n/a through 1.4.7.	6.5	More Details
CVE-2025-9376	The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection plugin for WordPress is vulnerable to unauthorized access of data due to an insufficient capability check on the 'stopbadbots_check_wordpress_logged_in_cookie' function in all versions up to, and including, 11.58. This makes it possible for unauthenticated attackers to bypass blocklists, rate limits, and other plugin functionality.	6.5	More Details
CVE-2025-48110	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mibuthu Link View allows Stored XSS. This issue affects Link View: from n/a through 0.8.0.	6.5	More Details
CVE-2025-54995	Asterisk is an open source private branch exchange and telephony toolkit. Prior to versions 18.26.4 and 18.9-cert17, RTP UDP ports and internal resources can leak due to a lack of session termination. This could result in leaks and resource exhaustion. This issue has been patched in versions 18.26.4 and 18.9-cert17.	6.5	More Details
CVE-2025-9217	The Slider Revolution plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 6.7.36 via the 'used_svg' and 'used_images' parameters. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-8977	The Simple Download Monitor plugin for WordPress is vulnerable to time-based SQL Injection via the order parameter in all versions up to, and including, 3.9.33 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, and permissions granted by an Administrator, 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-2025-48312	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 文派翻译 (WP Chinese Translation) WPAvatar allows Stored XSS. This issue affects WPAvatar: from n/a through 1.9.3.	6.5	More Details
CVE-2025-48356	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Isra Kanpress allows Stored XSS. This issue affects Kanpress: from n/a through 1.1.	6.5	More Details
CVE-2025-48354	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Smart Widgets Better Post & Filter Widgets for Elementor allows Stored XSS. This issue affects Better Post & Filter Widgets for Elementor: from n/a through 1.6.0.	6.5	More Details

CVE-2025-48315	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stanton119 WordPress HTML allows Stored XSS. This issue affects WordPress HTML: from n/a through 0.51.	6.5	More Details
CVE-2025-48316	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ItayXD Responsive Mobile-Friendly Tooltip allows Stored XSS. This issue affects Responsive Mobile-Friendly Tooltip: from n/a through 1.6.6.	6.5	More Details
CVE-2025-55750	Gitpod is a developer platform for cloud development environments. In versions before main-gha.33628 for both Gitpod Classic and Gitpod Classic Enterprise, OAuth integration with Bitbucket in certain conditions allowed a crafted link to expose a valid Bitbucket access token via the URL fragment when clicked by an authenticated user. This resulted from how Bitbucket returned tokens and how Gitpod handled the redirect flow. The issue was limited to Bitbucket (GitHub and GitLab integrations were not affected), required user interaction, and has been mitigated through redirect handling and OAuth logic hardening. The issue was resolved in main-gha.33628 and later. There are no workarounds.	6.5	More Details
CVE-2025-48322	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Finn Dohrn Statify Widget allows Stored XSS. This issue affects Statify Widget: from n/a through 1.4.6.	6.5	More Details
CVE-2025-48349	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in origincode Video Gallery – Vimeo and YouTube Gallery allows Stored XSS. This issue affects Video Gallery – Vimeo and YouTube Gallery: from n/a through 1.1.7.	6.5	More Details
CVE-2025-48347	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vincent Mimoun-Prat bxSlider integration for WordPress allows Stored XSS. This issue affects bxSlider integration for WordPress: from n/a through 1.7.2.	6.5	More Details
CVE-2021-4459	An authorized remote attacker can access files and directories outside the intended web root, potentially exposing sensitive system information of the affected Sunny Boy devices.	6.5	More Details
CVE-2025-58208	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in add-ons.org PDF for Elementor Forms + Drag And Drop Template Builder allows Stored XSS. This issue affects PDF for Elementor Forms + Drag And Drop Template Builder: from n/a through 6.2.0.	6.5	More Details
CVE-2025-25010	Incorrect authorization in Kibana can lead to privilege escalation via the built-in reporting_user role which incorrectly has the ability to access all Kibana Spaces.	6.5	More Details
CVE-2025-31972	HCL BigFix SM is affected by a Sensitive Information Exposure vulnerability where internal connections do not use TLS encryption which could allow an attacker unauthorized access to sensitive data transmitted between internal components.	6.5	More Details

CVE-2025-55495	Tenda AC6 V15.03.06.23_multi was discovered to contain a buffer overflow via the list parameter in the fromSetIpMacBind function.	6.5	More Details
CVE-2025-29364	spimsimulator spim v9.1.24 and before is vulnerable to Buffer Overflow in the READ_SYSCALL and WRITE_SYSCALL system calls. The application verifies the legitimacy of the starting and ending addresses for memory read/write operations. By configuring the starting and ending addresses for memory read/write to point to distinct memory segments within the virtual machine, it is possible to circumvent these checks.	6.5	More Details
CVE-2025-3601	An issue has been discovered in GitLab CE/EE affecting all versions from 8.15 before 18.1.5, 18.2 before 18.2.5, and 18.3 before 18.3.1 that could have could have allowed an authenticated user to cause a Denial of Service (DoS) condition by submitting URLs that generate excessively large responses.	6.5	More Details
CVE-2025-58213	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ameliabooking Booking System Trafft allows Stored XSS. This issue affects Booking System Trafft: from n/a through 1.0.14.	6.5	More Details
CVE-2025-58197	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mra13 / Team Tips and Tricks HQ Simple Download Monitor allows Stored XSS. This issue affects Simple Download Monitor: from n/a through 3.9.34.	6.5	More Details
CVE-2025-58211	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alexvtn Chatbox Manager allows Stored XSS. This issue affects Chatbox Manager: from n/a through 1.2.6.	6.5	More Details
CVE-2025-58196	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uicore UiCore Elements allows Stored XSS. This issue affects UiCore Elements: from n/a through 1.3.4.	6.5	More Details
CVE-2025-58195	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons allows Stored XSS. This issue affects Xpro Elementor Addons: from n/a through 1.4.17.	6.5	More Details
CVE-2025-58205	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Element Invader ElementInvader Addons for Elementor allows DOM-Based XSS. This issue affects ElementInvader Addons for Elementor: from n/a through 1.3.6.	6.5	More Details
CVE-2025-58198	Missing Authorization vulnerability in Xpro Xpro Theme Builder allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Xpro Theme Builder: from n/a through 1.2.9.	6.5	More Details
CVE-2025-58212	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in epeken Epeken All Kurir allows DOM-Based XSS. This issue affects Epeken All Kurir: from n/a through 2.0.1.	6.5	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in boldthemes Bold Page Builder allows	6.5	More

58194	Stored XSS. This issue affects Bold Page Builder: from n/a through 5.4.3.		Details
CVE-2025-54733	Missing Authorization vulnerability in Miles All Bootstrap Blocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects All Bootstrap Blocks: from n/a through 1.3.28.	6.5	More Details
CVE-2025-51968	A SQL Injection vulnerability exists in the action.php file of PuneethReddyHC Online Shopping System Advanced 1.0. The application fails to properly sanitize user-supplied input in the proId POST parameter, allowing attackers to inject arbitrary SQL expressions.	6.5	More Details
CVE-2025-51969	A SQL Injection vulnerability exists in the product.php page of PuneethReddyHC Online Shopping System Advanced 1.0. This flaw is present in the product_id GET parameter, which is not properly validated before being included in a SQL statement.	6.5	More Details
CVE-2025-58209	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rtCamp Transcoder allows Stored XSS. This issue affects Transcoder: from n/a through 1.4.0.	6.5	More Details
CVE-2025-7732	The Lazy Load for Videos plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its lazy-loading handlers in all versions up to, and including, 2.18.7 due to insufficient input sanitization and output escaping. The plugin’s JavaScript registration handlers read the client-supplied 'data-video-title' and 'href' attributes, decode HTML entities by default, and pass them directly into DOM sinks without any escaping or validation. 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-2025-8290	The List Subpages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title’ parameter in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8619	The OSM Map Widget for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Map Block URL in all versions up to, and including, 1.3.0 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-2025-9346	The Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings in all versions up to, and including, 10.14.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-9344	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'uwp_profile' and 'uwp_profile_header' shortcodes in all versions up to, and including, 1.2.42 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-2025-8603	The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 1.5.148 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-2025-8073	The Dynamic AJAX Product Filters for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘name’ parameter in all versions up to, and including, 1.3.7 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 injected page.	6.4	More Details
CVE-2025-6255	The Dynamic AJAX Product Filters for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘className’ parameter in all versions up to, and including, 1.3.7 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 injected page.	6.4	More Details
CVE-2025-53250	Server-Side Request Forgery (SSRF) vulnerability in Chartbeat Chartbeat allows Server Side Request Forgery. This issue affects Chartbeat: from n/a through 2.0.7.	6.4	More Details
CVE-2025-8150	The Events Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Typewriter and Countdown widgets in all versions up to, and including, 2.2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9651	A vulnerability was found in shafhasan chatbox up to 156a39cde62f78532c3265a70eda12c70907e56f. This impacts an unknown function of the file /chat.php. The manipulation of the argument user_id results in sql injection. The attack may be performed from a remote location. The exploit has been made public and could be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	6.3	More Details

CVE-2025-9654	A security flaw has been discovered in AiondaDotCom mcp-ssh up to 1.0.3. Affected by this issue is some unknown functionality of the file server-simple.mjs. Performing manipulation results in command injection. The attack can be initiated remotely. Upgrading to version 1.0.4 and 1.1.0 can resolve this issue. The patch is named cd2566a948b696501abfa6c6b03462cac5fb43d8. It is advisable to upgrade the affected component.	6.3	More Details
CVE-2025-9663	A vulnerability was identified in code-projects Simple Grading System 1.0. This impacts an unknown function of the file /edit_account.php of the component Admin Panel. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-9608	A vulnerability has been found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /module/FormulaMedia/view of the component Formula de Cálculo de Média Page. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-9609	A vulnerability was found in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /educacenso/consulta. The manipulation results in improper authorization. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-9580	A security vulnerability has been detected in LB-LINK BL-X26 1.2.8. This affects an unknown function of the file /goform/set_blacklist of the component HTTP Handler. Such manipulation of the argument mac leads to os command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9575	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This issue affects the function cgiMain of the file /cgi-bin/upload.cgi. Executing manipulation of the argument filename can lead to os command injection. The attack may be performed from a remote location. 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.	6.3	More Details
CVE-2025-9607	A flaw has been found in Portabilis i-Educar up to 2.10. Affected by this issue is some unknown functionality of the file /module/TabelaArredondamento/view of the component Tabelas de Arredondamento Page. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-9606	A vulnerability was detected in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /intranet/agenda_preferencias.php. Performing manipulation of the argument cod_agenda results in sql injection. The attack may be	6.3	More Details

	initiated remotely. The exploit is now public and may be used.		
CVE-2025-9603	A vulnerability was determined in Telesquare TLR-2005KSH 1.2.4. The affected element is an unknown function of the file /cgi-bin/internet.cgi?Command=lanCfg. Executing manipulation of the argument Hostname can lead to command injection. The attack may be performed from a remote location. 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.	6.3	More Details
CVE-2025-9602	A vulnerability was found in Xinhu RockOA up to 2.6.9. Impacted is the function publicsaveAjax of the file /index.php. Performing manipulation results in improper authorization. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-9586	A vulnerability was identified in Comfast CF-N1 2.6.0. This vulnerability affects the function wireless_device_dissoc of the file /usr/bin/webmgnt. Such manipulation of the argument mac leads to command injection. The attack may be performed from a remote location. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-9585	A vulnerability was determined in Comfast CF-N1 2.6.0. This affects the function wifilith_delete_pic_file of the file /usr/bin/webmgnt. This manipulation of the argument portal_delete_picname causes command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-9584	A vulnerability was found in Comfast CF-N1 2.6.0. Affected by this issue is the function update_interface_png of the file /usr/bin/webmgnt. The manipulation of the argument interface/display_name results in command injection. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-9582	A flaw has been found in Comfast CF-N1 2.6.0. Affected is the function ntp_timezone of the file /usr/bin/webmgnt. Executing manipulation of the argument timestr can lead to command injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-9581	A vulnerability was detected in Comfast CF-N1 2.6.0. This impacts the function multi_pppoe of the file /usr/bin/webmgnt. Performing manipulation of the argument phy_interface results in command injection. The attack may be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-9579	A weakness has been identified in LB-LINK BL-X26 1.2.8. The impacted element is an unknown function of the file /goform/set_hidessid_cfg of the component HTTP Handler. This manipulation of the argument enable causes os command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
	A vulnerability has been found in Comfast CF-N1 2.6.0. Affected by this		

CVE-2025-9583	vulnerability is the function ping_config of the file /usr/bin/webmgnt. The manipulation leads to command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-9664	A security flaw has been discovered in code-projects Simple Grading System 1.0. Affected is an unknown function of the file /add_student_grade.php of the component Admin Panel. The manipulation of the argument Add results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-9532	A flaw has been found in Portabilis i-Educar up to 2.10. This impacts an unknown function of the file /RegraAvaliacao/view. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9531	A vulnerability was detected in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /intranet/agenda.php of the component Agenda Module. Performing manipulation of the argument cod_agenda results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-51967	A Reflected Cross-site Scripting (XSS) vulnerability exists in the themeSet.php file of ProjectsAndPrograms School Management System 1.0. The application fails to sanitize user-supplied input in the theme POST parameter, allowing an attacker to inject and execute arbitrary JavaScript in a victim's browser.	6.1	More Details
CVE-2025-55579	SolidInvoice 2.3.7 and fixed in v.2.3.8 is vulnerable to Cross Site Scripting (XSS) in the Tax Rate functionality.	6.1	More Details
CVE-2025-50977	A template injection vulnerability leading to reflected cross-site scripting (XSS) has been identified in version 1.7.1, requiring authenticated admin access for exploitation. The vulnerability exists in the 'r' parameter and allows attackers to inject malicious Angular expressions that execute JavaScript code in the context of the application. The flaw can be exploited through GET requests to the summary endpoint as well as POST requests to specific Wicket interface endpoints, though the GET method provides easier weaponization. This vulnerability enables authenticated administrators to execute arbitrary client-side code, potentially leading to session hijacking, data theft, or further privilege escalation attacks.	6.1	More Details
CVE-2025-50978	In Gitblit v1.7.1, a reflected cross-site scripting (XSS) vulnerability exists in the way repository path names are handled. By injecting a specially crafted path payload an attacker can cause arbitrary JavaScript to execute when a victim views the manipulated URL. This flaw stems from insufficient input sanitization of filename elements.	6.1	More Details

CVE-2024-9648	The WP ULike Pro plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the WP_Ulike_Pro_File_Uploader class in all versions up to, and including, 1.9.3. This makes it possible for unauthenticated attackers to upload limited arbitrary files like .php2, .php6, .php7, .phps, .pht, .phtm, .pgif, .shtml, .phar, .inc, .hphp, .ctp, .module, .html, .svg on the affected site's server which may make make other attacks like Cross-Site Scripting possible. Only versions up to 1.8.7 were confirmed vulnerable, however, the earliest tested version for a patch we have access to is 1.9.4, so we are considering 1.9.4 the patched version.	6.1	More Details
CVE-2025-56236	FormCms v0.5.5 contains a stored cross-site scripting (XSS) vulnerability in the avatar upload feature. Authenticated users can upload .html files containing malicious JavaScript, which are accessible via a public URL. When a privileged user accesses the file, the script executes in their browser context.	6.1	More Details
CVE-2025-8897	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘'fl_builder' parameter in all versions up to, and including, 2.9.2.1 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-2025-55580	SolidInvoice 2.3.7 and v.2.3.8 is vulnerable to Cross Site Scripting (XSS) in the client's functionality.	6.1	More Details
CVE-2025-20295	A vulnerability in the CLI of Cisco UCS Manager Software could allow an authenticated, local attacker with administrative privileges to read or create a file or overwrite any file on the file system of the underlying operating system of an affected device, including system files. This vulnerability is due to insufficient input validation of command arguments supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to read or create a file or overwrite any file on the file system of the underlying operating system of the affected device, including system files. To exploit this vulnerability, the attacker must have valid administrative credentials on the affected device.	6.0	More Details
CVE-2024-13987	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in Synology RADIUS Server before 3.0.27-0139 allows remote authenticated users with administrator privileges to read or write limited files in SRM and conduct limited denial-of-service via unspecified vectors.	5.9	More Details
CVE-2025-48305	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vikingjs Goal Tracker for Patreon allows Stored XSS. This issue affects Goal Tracker for Patreon: from n/a through 0.4.6.	5.9	More Details
	Improper Neutralization of Input During Web Page Generation ('Cross-		

CVE-2025-48365	site Scripting') vulnerability in imaprogrammer Custom Comment allows Stored XSS. This issue affects Custom Comment: from n/a through 2.1.6.	5.9	More Details
CVE-2025-58216	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgwhite33 WP Thumbtack Review Slider allows Stored XSS. This issue affects WP Thumbtack Review Slider: from n/a through 2.6.	5.9	More Details
CVE-2025-48314	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in salubrio Add Code To Head allows Stored XSS. This issue affects Add Code To Head: from n/a through 1.17.	5.9	More Details
CVE-2025-48360	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Razvan Stanga Varnish/Nginx Proxy Caching allows Stored XSS. This issue affects Varnish/Nginx Proxy Caching: from n/a through 1.8.3.	5.9	More Details
CVE-2025-49035	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chaimchaikin Admin Menu Groups allows Stored XSS.This issue affects Admin Menu Groups: from n/a through 0.1.2.	5.9	More Details
CVE-2025-48323	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Md Abunaser Khan Advance Food Menu allows Stored XSS. This issue affects Advance Food Menu: from n/a through 1.0.	5.9	More Details
CVE-2025-49039	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mibuthu Link View allows Stored XSS.This issue affects Link View: from n/a through 0.8.0.	5.9	More Details
CVE-2025-48319	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gslauraspeck Mesa Mesa Reservation Widget allows Stored XSS. This issue affects Mesa Mesa Reservation Widget: from n/a through 1.0.0.	5.9	More Details
CVE-2025-48352	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sitesearch-yandex Yandex Site search pinger allows Stored XSS. This issue affects Yandex Site search pinger: from n/a through 1.5.	5.9	More Details
CVE-2025-48324	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in khashabawy tli.tl auto Twitter poster allows Stored XSS. This issue affects tli.tl auto Twitter poster: from n/a through 3.4.	5.9	More Details
CVE-2025-48313	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kevin heath Tripadvisor Shortcode allows Stored XSS. This issue affects Tripadvisor Shortcode: from n/a through 2.2.	5.9	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in everythingwp Risk Free Cash On Delivery		

2025-48358	(COD) – WooCommerce allows Stored XSS. This issue affects Risk Free Cash On Delivery (COD) – WooCommerce: from n/a through 1.0.4.	5.9	More Details
CVE-2025-56694	Client-side password validation (CWE-602) in lumasoft fotoShare Cloud 2025-03-13 allowing unauthenticated attackers to view password-protected photo albums.	5.8	More Details
CVE-2025-58049	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions from 14.4.2 to before 16.4.8, 16.5.0-rc-1 to before 16.10.7, and 17.0.0-rc-1 to before 17.4.0-rc-1, the PDF export jobs store sensitive cookies unencrypted in job statuses. XWiki shouldn't store passwords in plain text, and it shouldn't be possible to gain access to plain text passwords by gaining access to, e.g., a backup of the data directory. This vulnerability has been patched in XWiki 16.4.8, 16.10.7, and 17.4.0-rc-1.	5.8	More Details
CVE-2025-54734	Missing Authorization vulnerability in bPlugins B Slider allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects B Slider: from n/a through 1.1.30.	5.8	More Details
CVE-2025-2246	An issue has been discovered in GitLab CE/EE affecting all versions before 18.1.5, 18.2 before 18.2.5, and 18.3 before 18.3.1 that could have allowed unauthenticated users to access sensitive manual CI/CD variables by querying the GraphQL API.	5.8	More Details
CVE-2025-50985	diskover-web v2.3.0 Community Edition is vulnerable to multiple reflected cross-site scripting (XSS) flaws in its web interface. Unsanitized GET parameters including maxage, maxindex, index, path, q (query), and doctype are directly echoed into the HTML response, allowing attackers to inject and execute arbitrary JavaScript when a victim visits a maliciously crafted URL.	5.6	More Details
CVE-2025-50986	diskover-web v2.3.0 Community Edition suffers from multiple stored cross-site scripting (XSS) vulnerabilities in its administrative settings interface. Various configuration fields such as ES_HOST, ES_INDEXREFRESH, ES_PORT, ES_SCROLLSIZE, ES_TRANSLOGSIZE, ES_TRANSLOGSYNCINT, EXCLUDES_FILES, FILE_TYPES[], INCLUDES_DIRS, INCLUDES_FILES, and TIMEZONE do not properly sanitize user-supplied input. Malicious payloads submitted via these parameters are persisted in the application and executed whenever an administrator views or edits the settings page.	5.6	More Details
CVE-2025-58335	In JetBrains Junie before 252.284.66, 251.284.66, 243.284.66, 252.284.61, 251.284.61, 243.284.61, 252.284.50, 252.284.54, 251.284.54, 251.284.50, 243.284.54, 243.284.50 information disclosure was possible via search_project function	5.5	More Details
CVE-	OpenEBS Local PV RawFile allows dynamic deployment of Stateful Persistent Node-Local Volumes & Filesystems for Kubernetes. Prior to version 0.10.0, persistent volume data is world readable and that would allow non-privileged users to access sensitive data such as databases of k8s workload. The rawfile-localpv storage class creates persistent volume data under /var/csi/rawfile/ on Kubernetes hosts by default.		

2025-58061	However, the directory and data in it are world-readable. It allows non-privileged users to access the whole persistent volume data, and those can include sensitive information such as a whole database if the Kubernetes tenants are running MySQL or PostgreSQL in a container so it could lead to a database breach. This issue has been patched in version 0.10.0.	5.5	More Details
CVE-2025-20290	A vulnerability in the logging feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches, Cisco Nexus 9000 Series Switches in standalone NX-OS mode, Cisco UCS 6400 Fabric Interconnects, Cisco UCS 6500 Series Fabric Interconnects, and Cisco UCS 9108 100G Fabric Interconnects could allow an authenticated, local attacker access to sensitive information. This vulnerability is due to improper logging of sensitive information. An attacker could exploit this vulnerability by accessing log files on the file system where they are stored. A successful exploit could allow the attacker to access sensitive information, such as stored credentials.	5.5	More Details
CVE-2025-43284	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.7.7, macOS Ventura 13.7.7, macOS Sequoia 15.6. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2024-54554	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-49790	IBM Watson Studio on Cloud Pak for Data 4.0 and 5.0 is vulnerable to 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.	5.4	More Details
CVE-2025-20342	A vulnerability in the Virtual Keyboard Video Monitor (vKVM) connection handling of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker with low privileges to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid user credentials with privileges that allow for vKVM access on the affected device. Note: The affected vKVM client is also included in Cisco UCS Manager.	5.4	More Details
CVE-2025-51971	A reflected Cross-Site Scripting (XSS) vulnerability exists in register.php of PuneethReddyHC Online Shopping System Advanced 1.0. Unsanitized user input in the f_name parameter is reflected in the server response without proper HTML encoding or output escaping. This allows remote attackers to inject arbitrary JavaScript code.	5.4	More Details

CVE-2025-48357	Cross-Site Request Forgery (CSRF) vulnerability in Theme Century Century ToolKit allows Cross Site Request Forgery. This issue affects Century ToolKit: from n/a through 1.2.1.	5.4	More Details
CVE-2025-48362	Cross-Site Request Forgery (CSRF) vulnerability in Saeed Sattar Beglou Hesabfa Accounting allows Cross Site Request Forgery. This issue affects Hesabfa Accounting: from n/a through 2.2.4.	5.4	More Details
CVE-2025-31979	A File Upload Validation Bypass vulnerability has been identified in the HCL BigFix SM, where the application fails to properly enforce file type restrictions during the upload process. An attacker may exploit this flaw to upload malicious or unauthorized files, such as scripts, executables, or web shells, by bypassing client-side or server-side validation mechanisms.	5.4	More Details
CVE-2025-9650	A vulnerability has been found in yeqifu carRental up to 3fabb7eae93d209426638863980301d6f99866b3. This affects the function removeFileByPath of the file src/main/java/com/yeqifu/sys/utils/AppFileUtils.java. The manipulation of the argument carimg leads to path traversal. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. This product adopts a rolling release strategy to maintain continuous delivery	5.4	More Details
CVE-2025-53337	Missing Authorization vulnerability in Ashan Perera LifePress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects LifePress: from n/a through 2.1.3.	5.4	More Details
CVE-2025-20347	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard and Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to view sensitive information or upload and modify files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit th vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions, such as accessing sensitive information regarding HTTP Proxy and NTP configurations, uploading images, and damaging image files on an affected device.	5.4	More Details
CVE-2025-9352	The Pronamic Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the description field in all versions up to, and including, 2.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-31977	HCL BigFix SM is affected by cryptographic weakness due to weak or outdated encryption algorithms. An attacker with network access could exploit this weakness to decrypt or manipulate encrypted communications under certain conditions.	5.3	More Details
	diskover-web v2.3.0 Community Edition is vulnerable to multiple		

CVE-2025-50984	boolean-based blind SQL injection flaws in its Elasticsearch configuration form. Unsanitized user input in POST parameters such as ES_PASS, ES_MAXSIZE, ES_TRANSLOGSIZE, ES_TIMEOUT, ES_USER, ES_HOST, ES_PORT, ES_SCROLLSIZE, ES_CHUNKSIZE and others can be crafted to inject arbitrary SQLite expressions wrapped in JSON functions. By exploiting these injection points, an attacker can infer or extract sensitive information from the underlying database without authentication. This issue stems from improper input validation and parameterization in the application's JSON-based query construction.	5.3	More Details
CVE-2025-52054	An issue was discovered in Tenda AC8 v4.0 AC1200 Dual-band Gigabit Wireless Router AC8v4.0 Firmware 16.03.33.05. The root password of the device is calculated with a static string and the last two octets of the MAC address of the device. This allows an unauthenticated attacker to authenticate with network services on the device.	5.3	More Details
CVE-2025-48081	Path Traversal: '.../...//' vulnerability in Printeers Printeers Print & Ship allows Path Traversal.This issue affects Printeers Print & Ship: from n/a through 1.17.0.	5.3	More Details
CVE-2025-4225	An issue has been discovered in GitLab CE/EE affecting all versions from 14.1 before 18.1.5, 18.2 before 18.2.5, and 18.3 before 18.3.1 that that under certain conditions could have allowed an unauthenticated attacker to cause a denial-of-service condition affecting all users by sending specially crafted GraphQL requests.	5.3	More Details
CVE-2025-54877	Tuleap is an Open Source Suite created to facilitate management of software development and collaboration. In Tuleap Community Edition versions before 16.10.99.1754050155 and Tuleap Enterprise Edition versions before 16.9-8 and before 16.10-5, an attacker can access to the content of the special and always there fields of accessible artifacts even if the permissions associated with the underlying fields do not allow it. This issue has been fixed in Tuleap Community Edition version 16.10.99.1754050155 and Tuleap Enterprise Edition versions 16.9-8 and 16.10-5.	5.3	More Details
CVE-2025-57220	An input validation flaw in the 'ate' service of Tenda AC10 v4.0 firmware v16.03.10.09_multi_TDE01 to escalate privileges to root via a crafted UDP packet.	5.3	More Details
CVE-2025-57219	Incorrect access control in the endpoint /goform/ate of Tenda AC10 v4.0 firmware v16.03.10.09_multi_TDE01 allows attackers to escalate privileges or access sensitive components via a crafted request.	5.3	More Details
CVE-2025-57756	Contao is an Open Source CMS. In versions starting from 4.9.14 and prior to 4.13.56, 5.3.38, and 5.6.1, protected content elements that are rendered as fragments are indexed and become publicly available in the front end search. This issue has been patched in versions 4.13.56, 5.3.38, and 5.6.1. A workaround involves disabling the front end search.	5.3	More Details
CVE-2025-	Contao is an Open Source CMS. In versions starting from 5.0.0 and prior to 5.3.38 and 5.6.1, if a news feed contains protected news archives, their news items are not filtered and become publicly available in the	5.3	More

57757	RSS feed. This issue has been patched in versions 5.3.38 and 5.6.1. A workaround involves not adding protected news archives to the news feed page.		Details
CVE-2025-58058	xz is a pure golang package for reading and writing xz-compressed files. Prior to version 0.5.14, it is possible to put data in front of an LZMA-encoded byte stream without detecting the situation while reading the header. This can lead to increased memory consumption because the current implementation allocates the full decoding buffer directly after reading the header. The LZMA header doesn't include a magic number or has a checksum to detect such an issue according to the specification. Note that the code recognizes the issue later while reading the stream, but at this time the memory allocation has already been done. This issue has been patched in version 0.5.14.	5.3	More Details
CVE-2025-57217	Tenda AC10 v4.0 firmware v16.03.10.09_multi_TDE01 was discovered to contain a stack overflow via the Password parameter in the function R7WebsSecurityHandler.	5.3	More Details
CVE-2025-39246	There is an Unquoted Service Path Vulnerability in some HikCentral FocSign versions. This could allow an authenticated user to potentially enable escalation of privilege via local access.	5.3	More Details
CVE-2025-9619	A security flaw has been discovered in E4 Sistemas Mercatus ERP 2.00.019. The affected element is an unknown function of the file /basico/webservice/imprimir-danfe/id/. Performing manipulation results in improper control of resource identifiers. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-58201	Missing Authorization vulnerability in AfterShip & Automizely AfterShip Tracking allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects AfterShip Tracking: from n/a through 1.17.17.	5.3	More Details
CVE-2025-57218	Tenda AC10 v4.0 firmware v16.03.10.09_multi_TDE01 was discovered to contain a stack overflow via the security_5g parameter in the function sub_46284C.	5.3	More Details
CVE-2025-48327	Missing Authorization vulnerability in inkthemes WP Mailgun SMTP allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WP Mailgun SMTP: from n/a through 1.0.7.	5.3	More Details
CVE-2025-48361	Insertion of Sensitive Information Into Sent Data vulnerability in Saeed Sattar Beglou Hesabfa Accounting allows Retrieve Embedded Sensitive Data. This issue affects Hesabfa Accounting: from n/a through 2.2.4.	5.3	More Details
CVE-2025-7956	The Ajax Search Lite plugin for WordPress is vulnerable to Basic Information Exposure due to missing authorization in its AJAX search handler in all versions up to, and including, 4.13.1. This makes it possible for unauthenticated attackers to issue repeated AJAX requests to leak the content of any protected post in rolling 100-character windows.	5.3	More Details
CVE-	AIML Solutions for HCL SX is vulnerable to a URL validation vulnerability. The issue may allow attackers to launch a server-side		

2025-31971	request forgery (SSRF) attack enabling unauthorized network calls from the system, potentially exposing internal services or sensitive information.	5.1	More Details
CVE-2025-20262	A vulnerability in the Protocol Independent Multicast Version 6 (PIM6) feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, low-privileged, remote attacker to trigger a crash of the PIM6 process, resulting in a denial of service (DoS) condition. This vulnerability is due to improper processing of PIM6 ephemeral data queries. An attacker could exploit this vulnerability by sending a crafted ephemeral query to an affected device through one of the following methods: NX-API REST, NETCONF, RESTConf, gRPC, or Model Driven Telemetry. A successful exploit could allow the attacker to cause the PIM6 process to crash and restart, causing potential adjacency flaps and resulting in a DoS of the PIM6 and ephemeral query processes.	5.0	More Details
CVE-2025-20348	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard and Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to view sensitive information or upload and modify files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit th vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions, such as accessing sensitive information regarding HTTP Proxy and NTP configurations, uploading images, and damaging image files on an affected device.	5.0	More Details
CVE-2025-5101	An issue has been discovered in GitLab CE/EE affecting all versions before 18.1.5, 18.2 before 18.2.5, and 18.3 before 18.3.1 that under certain conditions could have allowed an authenticated attacker to distribute malicious code that appears harmless in the web interface by taking advantage of ambiguity between branches and tags during repository imports.	5.0	More Details
CVE-2025-9345	The File Manager, Code Editor, and Backup by Managefy plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.4.8 via the ajax_downloadfile() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform actions on files outside of the originally intended directory.	4.9	More Details
CVE-2025-48364	Server-Side Request Forgery (SSRF) vulnerability in vEnCa-X rajce allows Server Side Request Forgery. This issue affects rajce: from n/a through 0.4.2.	4.9	More Details
CVE-2025-58204	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Eric Teubert Podlove Podcast Publisher allows Phishing. This issue affects Podlove Podcast Publisher: from n/a through 4.2.5.	4.7	More Details
CVE-2025-	There is a CSV Injection Vulnerability in some HikCentral Master Lite versions. This could allow an attacker to inject executable commands	4.7	More

39245	via malicious CSV data.		Details
CVE-2025-9528	A vulnerability was determined in Linksys E1700 1.0.0.4.003. This vulnerability affects the function systemCommand of the file /goform/systemCommand. Executing manipulation of the argument command can lead to os command injection. The attack may be launched remotely. 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.	4.7	More Details
CVE-2025-20292	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute a command injection attack on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by entering crafted input as the argument of an affected CLI command. A successful exploit could allow the attacker to read and write files on the underlying operating system with the privileges of a non-root user account. File system access is limited to the permissions that are granted to that non-root user account.	4.4	More Details
CVE-2025-9195	Improper input validation in firmware of some Solidigm DC Products may allow an attacker with local access to cause a Denial of Service	4.4	More Details
CVE-2025-58203	Server-Side Request Forgery (SSRF) vulnerability in solacewp Solace Extra allows Server Side Request Forgery. This issue affects Solace Extra: from n/a through 1.3.2.	4.4	More Details
CVE-2025-8490	The All-in-One WP Migration and Backup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Import in all versions up to, and including, 7.97 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-2025-48310	Cross-Site Request Forgery (CSRF) vulnerability in wptableeditor Table Editor allows Cross Site Request Forgery. This issue affects Table Editor: from n/a through 1.6.4.	4.3	More Details
CVE-2025-48350	Missing Authorization vulnerability in Neuralabz LTD AutoWP allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AutoWP: from n/a through 2.2.2.	4.3	More Details
CVE-2025-0951	Multiple plugins and/or themes for WordPress by LiquidThemes are vulnerable to unauthorized access due to a missing capability check on the liquid_reset_wordpress_before AJAX in various versions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to deactivate all of a site's plugins. While we escalated this to Envato after not being able to establish contact, it appears the developer added a nonce check, however that is not sufficient	4.3	More Details

	protection as the nonce is exposed to all users with access to the dashboard.		
CVE-2025-58192	Missing Authorization vulnerability in Xylus Themes WP Bulk Delete allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Bulk Delete: from n/a through 1.3.6.	4.3	More Details
CVE-2025-58193	Missing Authorization vulnerability in Uncanny Owl Uncanny Automator allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Uncanny Automator: from n/a through 6.7.0.1.	4.3	More Details
CVE-2025-9647	A weakness has been identified in mtons mblog up to 3.5.0. This issue affects some unknown processing of the file /admin/role/list. This manipulation of the argument Name causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-48318	Cross-Site Request Forgery (CSRF) vulnerability in shen2 多说社会化评论框 allows Cross Site Request Forgery. This issue affects 多说社会化评论框: from n/a through 1.2.	4.3	More Details
CVE-2025-58202	Cross-Site Request Forgery (CSRF) vulnerability in Plugins and Snippets Simple Page Access Restriction allows Cross Site Request Forgery. This issue affects Simple Page Access Restriction: from n/a through 1.0.32.	4.3	More Details
CVE-2025-49040	Cross-Site Request Forgery (CSRF) vulnerability in Backup Bolt allows Cross Site Request Forgery.This issue affects Backup Bolt: from n/a through 1.4.1.	4.3	More Details
CVE-2025-48363	Cross-Site Request Forgery (CSRF) vulnerability in Metin Saraç Popup for CF7 with Sweet Alert allows Cross Site Request Forgery. This issue affects Popup for CF7 with Sweet Alert: from n/a through 1.6.5.	4.3	More Details
CVE-2024-54568	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.2. Parsing a maliciously crafted file may lead to an unexpected app termination.	4.3	More Details
CVE-2025-9595	A vulnerability was found in code-projects Student Information Management System 1.0. The impacted element is an unknown function of the file /login.php. The manipulation of the argument uname results in cross site scripting. The attack may be performed from a remote location. The exploit has been made public and could be used.	4.3	More Details
CVE-2025-48348	Incorrect Privilege Assignment vulnerability in chandrashekharsahu Site Offline allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Site Offline: from n/a through 1.5.7.	4.3	More Details
CVE-2025-57759	Contao is an Open Source CMS. In versions starting from 5.3.0 and prior to 5.3.38 and 5.6.1, under certain conditions, back end users may be able to edit fields of pages and articles without having the necessary permissions. This issue has been patched in versions 5.3.38 and 5.6.1. There are no workarounds.	4.3	More Details
CVE-	A security vulnerability has been detected in PHPGurukul Directory Management System 2.0. This vulnerability affects unknown code of the		

2025-9656	file /admin/add-directory.php. The manipulation of the argument fullname leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-8147	The LWSCache plugin for WordPress is vulnerable to unauthorized modification of data due to improper authorization on the lwscache_activatePlugin() function in all versions up to, and including, 2.8.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate arbitrary whitelisted LWS plugins.	4.3	More Details
CVE-2025-57758	Contao is an Open Source CMS. In versions starting from 5.0.0 and prior to 5.3.38 and 5.6.1, the table access voter in the back end doesn't check if a user is allowed to access the corresponding module. This issue has been patched in versions 5.3.38 and 5.6.1. A workaround involves not relying solely on the voter and additionally to check USER_CAN_ACCESS_MODULE.	4.3	More Details
CVE-2025-9374	The Ultimate Tag Warrior Importer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.2. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to import tags granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-57821	Basecamp's Google Sign-In adds Google sign-in to Rails applications. Prior to version 1.3.0, it is possible to craft a malformed URL that passes the "same origin" check, resulting in the user being redirected to another origin. Rails applications configured to store the flash information in a session cookie may be vulnerable, if this can be chained with an attack that allows injection of arbitrary data into the session cookie. This issue has been patched in version 1.3.0. If upgrading is not possible at this time, a way to mitigate the chained attack can be done by explicitly setting SameSite=Lax or SameSite=Strict on the application session cookie.	4.2	More Details
CVE-2025-54142	Akamai Ghost before 2025-07-21 allows HTTP Request Smuggling via an OPTIONS request that has an entity body, because there can be a subsequent request within the persistent connection between an Akamai proxy server and an origin server, if the origin server violates certain Internet standards.	4.0	More Details
CVE-2025-9513	A flaw has been found in editso fuso up to 1.0.4-beta.7. This affects the function PenetrateRsaAndAesHandshake of the file src/net/penetrate/handshake/mod.rs. This manipulation of the argument priv_key causes inadequate encryption strength. Remote exploitation of the attack is possible. A high degree of complexity is needed for the attack. The exploitability is reported as difficult.	3.7	More Details
	A vulnerability was identified in coze-studio up to 0.2.4. The impacted element is an unknown function of the file backend/domain/plugin/encrypt/aes.go. The manipulation of the		

CVE-2025-9604	argument AuthSecretKey/StateSecretKey/OAuthTokenSecretKey leads to use of hard-coded cryptographic key . It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is regarded as difficult. To fix this issue, it is recommended to deploy a patch. The vendor replied to the GitHub issue (translated from simplified Chinese): "For scenarios requiring encryption, we will implement user-defined key management through configuration and optimize the use of encryption tools, such as random salt."	3.7	More Details
CVE-2025-9514	A vulnerability has been found in macrozheng mall up to 1.0.3. This impacts an unknown function of the component Registration. Such manipulation leads to weak password requirements. The attack can be executed remotely. Attacks of this nature are highly complex. The exploitability is said to be difficult. The vendor deleted the GitHub issue for this vulnerability without and explanation.	3.7	More Details
CVE-2025-9659	A vulnerability has been found in O2OA up to 10.0-410. The affected element is an unknown function of the file /x_portal_assemble_designer/jaxrs/widget of the component Personal Profile Page. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor replied in the GitHub issue (translated from simplified Chinese): "This issue will be fixed in the new version."	3.5	More Details
CVE-2025-9657	A vulnerability was detected in O2OA up to 10.0-410. This issue affects some unknown processing of the file /x_program_center/jaxrs/script of the component Personal Profile Page. The manipulation of the argument name/alias/description results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used. The vendor replied in the GitHub issue (translated from simplified Chinese): "This issue will be fixed in the new version."	3.5	More Details
CVE-2025-9590	A vulnerability was identified in Weaver E-Mobile Mobile Management Platform up to 20250813. Affected by this vulnerability is an unknown functionality. The manipulation of the argument gohome leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-9658	A flaw has been found in O2OA up to 10.0-410. Impacted is an unknown function of the file /x_portal_assemble_designer/jaxrs/dict/ of the component Personal Profile Page. This manipulation of the argument name/alias/description causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor replied in the GitHub issue (translated from simplified Chinese): "This issue will be fixed in the new version."	3.5	More Details
CVE-2025-9653	A vulnerability was identified in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /intranet/educar_projeto_cad.php of the component Cadastrar projeto Page. Such manipulation of the argument nome/observacao leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	3.5	More Details

CVE-2025-9652	A vulnerability was determined in Portabilis i-Educar up to 2.10. Affected is an unknown function of the file /intranet/educar_transferencia_tipo_cad.php of the component Cadastrar tipo de transferência Page. This manipulation of the argument nm_tipo/desc_tipo causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	3.5	More Details
CVE-2025-9646	A security flaw has been discovered in O2OA up to 10.0-410. This vulnerability affects unknown code of the file /x_organization_assemble_personal/jaxrs/definition/calendarConfig. The manipulation of the argument toMonthViewName results in cross site scripting. The attack can be launched remotely. The exploit has been released to the public and may be exploited. The vendor replied in the GitHub issue (translated from simplified Chinese): "This issue will be fixed in the new version."	3.5	More Details
CVE-2025-9655	A weakness has been identified in O2OA up to 10.0-410. This affects an unknown part of the file /x_organization_assemble_control/jaxrs/person/ of the component Personal Profile Page. Executing manipulation of the argument Description can lead to cross site scripting. The attack can be launched remotely. The vendor replied in the GitHub issue (translated from simplified Chinese): "This issue will be fixed in the new version."	3.5	More Details
CVE-2025-48979	An Improper Input Validation in UISP Application could allow a Command Injection by a malicious actor with High Privileges and local access.	3.4	More Details
CVE-2025-9649	A security vulnerability has been detected in appneta tcpreplay 4.5.1. Impacted is the function calc_sleep_time of the file send_packets.c. Such manipulation leads to divide by zero. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. Upgrading to version 4.5.3-beta3 is recommended to address this issue. It is advisable to upgrade the affected component. The vendor confirms in a GitHub issue reply: "Was able to reproduce in 6fcbf03 but NOT 4.5.3-beta3."	3.3	More Details
CVE-2024-44271	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2. An app may be able to record the screen without an indicator.	3.3	More Details
CVE-2025-43255	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.7.7, macOS Sequoia 15.6, macOS Ventura 13.7.7. An app may be able to cause unexpected system termination.	3.3	More Details
CVE-2025-9577	A security flaw has been discovered in TOTOLINK X2000R up to 2.0.0. The affected element is an unknown function of the file /etc/shadow.sample of the component Administrative Interface. The manipulation results in use of default credentials. Attacking locally is a requirement. Attacks of this nature are highly complex. The exploitability is described as difficult. The exploit has been released to the public and may be exploited.	2.5	More Details

CVE-2025-9589	A vulnerability was determined in Cudy WR1200EA 2.3.7-20250113-121810. Affected is an unknown function of the file /etc/shadow. Executing manipulation can lead to use of default password. The attack needs to be launched locally. A high complexity level is associated with this attack. The exploitability is told to be difficult. 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.	2.5	More Details
CVE-2025-9576	A vulnerability was identified in seeedstudio ReSpeaker LinkIt7688. Impacted is an unknown function of the file /etc/shadow of the component Administrative Interface. The manipulation leads to use of default credentials. An attack has to be approached locally. A high degree of complexity is needed for the attack. The exploitability is considered 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.	2.5	More Details
CVE-2025-51643	Meitrack T366G-L GPS Tracker devices contain an SPI flash chip (Winbond 25Q64JVSIQ) that is accessible without authentication or tamper protection. An attacker with physical access to the device can use a standard SPI programmer to extract the firmware using flashrom. This results in exposure of sensitive configuration data such as APN credentials, backend server information, and network parameter	2.4	More Details
CVE-2025-9591	A security vulnerability has been detected in ZrLog up to 3.1.5. This vulnerability affects unknown code of the file /api/admin/template/config of the component Theme Configuration Form. Such manipulation of the argument footerLink leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-4644	A Session Fixation vulnerability existed in Payload's SQLite adapter due to identifier reuse during account creation. A malicious attacker could create a new account, save its JSON Web Token (JWT), and then delete the account, which did not invalidate the JWT. As a result, the next newly created user would receive the same identifier, allowing the attacker to reuse the JWT to authenticate and perform actions as that user. This issue has been fixed in version 3.44.0 of Payload.	N/A	More Details
CVE-2025-55202	Opencast is a free, open-source platform to support the management of educational audio and video content. In version 18.0 and versions before 17.7, the protections against path traversal attacks in the UI config module are insufficient, still partially allowing for attacks in very specific cases. The path is checked without checking for the file separator. This could allow attackers access to files within another folder which starts with the same path. This issue has been fixed in versions 17.7 and 18.1. To mitigate this issue, check for folders that start with the same path as the ui-config folder.	N/A	More Details
CVE-	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent.		More

2025-40703	The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/group" petition, "name" and "alias-0" parameters.	N/A	Details
CVE-2025-40702	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/file" petition, "creator" and "license_holder" parameters.	N/A	More Details
CVE-2025-30038	The vulnerability consists of a session ID leak when saving a file downloaded from CGM CLININET. The identifier is exposed through a built-in Windows security feature that stores additional metadata in an NTFS alternate data stream (ADS) for all files downloaded from potentially untrusted sources.	N/A	More Details
CVE-2025-30039	Unauthenticated access to the "/cgi-bin/CliniNET.prd/GetActiveSessions.pl" endpoint allows takeover of any user session logged into the system, including users with admin privileges.	N/A	More Details
CVE-2025-9071	Erroneously using an all-zero seed for RSA-OEAP padding instead of the generated random bytes, in Oberon microsystems AG's Oberon PSA Crypto library in all versions up to 1.5.1, results in deterministic RSA and thus in a loss of confidentiality for guessable messages, recognition of repeated messages, and loss of security proofs.	N/A	More Details
CVE-2025-7383	Padding oracle attack vulnerability in Oberon microsystem AG's Oberon PSA Crypto library in all versions since 1.0.0 and prior to 1.5.1 allows an attacker to recover plaintexts via timing measurements of AES-CBC PKCS#7 decrypt operations.	N/A	More Details
CVE-2025-7071	Padding oracle attack vulnerability in Oberon microsystem AG's ocrypto library in all versions since 3.1.0 and prior to 3.9.2 allows an attacker to recover plaintexts via timing measurements of AES-CBC PKCS#7 decrypt operations.	N/A	More Details
CVE-2025-4643	Payload uses JSON Web Tokens (JWT) for authentication. After log out JWT is not invalidated, which allows an attacker who has stolen or intercepted token to freely reuse it until expiration date (which is by default set to 2 hours, but can be changed). This issue has been fixed in version 3.44.0 of Payload.	N/A	More Details
CVE-2025-29879	A NULL pointer dereference vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.4907 and later	N/A	More Details
CVE-2025-30040	The vulnerability allows unauthenticated users to download a file containing session ID data by directly accessing the "/cgi-bin/CliniNET.prd/utils/userlogxls.pl" endpoint.	N/A	More Details

CVE-2025-55175	QuickCMS is vulnerable to Reflected XSS via sLangEdit parameter in admin's panel functionality. A malicious attacker can craft a specially crafted URL that, when opened, results in arbitrary JavaScript execution in the victim's browser. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-54777	Uncaught exception issue exists in Multiple products in bizhub series. If a malformed file is imported as an S/MIME Email certificate, it may cause a denial-of-service issue that disable the Web Connection feature.	N/A	More Details
CVE-2025-30041	The paths "/cgi-bin/CliniNET.prd/utils/userlogstat.pl", "/cgi-bin/CliniNET.prd/utils/usrlogstat.pl", and "/cgi-bin/CliniNET.prd/utils/dblogstat.pl" expose data containing session IDs.	N/A	More Details
CVE-2025-57797	Incorrect privilege assignment vulnerability exists in ScanSnap Manager installers versions prior to V6.5L61. If this vulnerability is exploited, an authenticated local attacker may escalate privileges and execute an arbitrary command.	N/A	More Details
CVE-2025-30048	The "serverConfig" endpoint, which returns the module configuration including credentials, is accessible without authentication.	N/A	More Details
CVE-2025-30055	The "system" function receives untrusted input from the user. If the "EnableJSCaching" option is enabled, it is possible to execute arbitrary code provided as the "Module" parameter.	N/A	More Details
CVE-2025-5808	Improper Input Validation vulnerability in OpenText Self Service Password Reset allows Authentication Bypass.This issue affects Self Service Password Reset from before 4.8 patch 3.	N/A	More Details
CVE-2024-12923	A cross-site scripting (XSS) vulnerability has been reported to affect Photo Station. If a remote attacker gains a user account, they can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following version: Photo Station 6.4.5 (2025/01/02) and later	N/A	More Details
CVE-2025-57846	Multiple i-フィルター products contain an issue with incorrect default permissions. If this vulnerability is exploited, a local authenticated attacker may replace a service executable on the system where the product is running, potentially allowing arbitrary code execution with SYSTEM privileges.	N/A	More Details
CVE-2025-40704	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/edition" petition, "name" parameter.	N/A	More Details
	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the		

CVE-2025-40705	Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/acquisition" petition, "name" parameter.	N/A	More Details
CVE-2025-53507	Multiple products provided by iND Co.,Ltd contain an insecure storage of sensitive information vulnerability. If exploited, configuration information, such as admin password, may be disclosed. As for the details of affected product names and versions, refer to the information under [Product Status].	N/A	More Details
CVE-2025-29878	A NULL pointer dereference vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.4907 and later	N/A	More Details
CVE-2025-54080	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. An out-of-bounds read was found in Exiv2 versions 0.28.5 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. The bug is fixed in version 0.28.6.	N/A	More Details
CVE-2025-55304	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. A denial-of-service was found in Exiv2 version 0.28.5: a quadratic algorithm in the ICC profile parsing code in jpegBase::readMetadata() can cause Exiv2 to run for a long time. The denial-of-service is triggered when Exiv2 is used to read the metadata of a crafted jpg image file. The bug is fixed in version 0.28.6.	N/A	More Details
CVE-2024-46916	Diebold Nixdorf Vynamic Security Suite through 4.3.0 SR06 contains functionality that allows the removal of critical system files before the filesystem is properly mounted (e.g., leveraging a delete call in /etc/rc.d/init.d/mountfs to remove the /etc/fstab file). This can allow code execution and, in some versions, enable recovery of TPM Disk Encryption keys and decryption of the Windows system partition.	N/A	More Details
CVE-2025-2313	In the Print.pl service, the "uhcPrintServerPrint" function allows execution of arbitrary code via the "CopyCounter" parameter.	N/A	More Details
CVE-2025-29875	A NULL pointer dereference vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.4907 and later	N/A	More Details

CVE-2025-30036	Stored XSS vulnerability exists in the "Oddział" (Ward) module, in the death diagnosis description field, and allows the execution of arbitrary JavaScript code. This can lead to session hijacking of other users and potentially to privilege escalation up to full administrative rights.	N/A	More Details
CVE-2024-46917	Diebold Nixdorf Vynamic Security Suite through 4.3.0 SR01 does not validate file attributes or the contents of /root during integrity validation. This allows code execution, recovery of TPM Disk Encryption keys, decryption of the Windows system partition, and full control of the Windows OS, e.g., through ~/.profile changes.	N/A	More Details
CVE-2025-29874	A NULL pointer dereference vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.4907 and later	N/A	More Details
CVE-2025-30037	The system exposes several endpoints, typically including "/int/" in their path, that should be restricted to internal services, but are instead publicly accessible without authentication to any host able to reach the application server on port 443/tcp.	N/A	More Details
CVE-2025-47909	Hosts listed in TrustedOrigins implicitly allow requests from the corresponding HTTP origins, allowing network MitMs to perform CSRF attacks. After the CVE-2025-24358 fix, a network attacker that places a form at http://example.com can't get it to submit to https://example.com because the Origin header is checked with sameOrigin against a synthetic URL. However, if a host is added to TrustedOrigins, both its HTTP and HTTPS origins will be allowed, because the schema of the synthetic URL is ignored and only the host is checked. For example, if an application is hosted on https://example.com and adds example.net to TrustedOrigins, a network attacker can serve a form at http://example.net to perform the attack. Applications should migrate to net/http.CrossOriginProtection, introduced in Go 1.25. If that is not an option, a backport is available as a module at filippo.io/csrf, and a drop-in replacement for the github.com/gorilla/csrf API is available at filippo.io/csrf/gorilla.	N/A	More Details
CVE-2025-40709	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/person/<ID>” petition, "name" and "alias-0” parameters.	N/A	More Details
CVE-2025-40708	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/event" petition, "name" parameter.	N/A	More Details

CVE-2025-22483	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following versions: License Center 1.8.51 and later License Center 1.9.51 and later	N/A	More Details
CVE-2025-40707	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/place" petition, "name" and "alias-0" parameters.	N/A	More Details
CVE-2025-40706	Cross-Site Scripting (XSS) vulnerability in OpenAtlas v8.9.0 from the Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH), due to inadequate validation of user input when a POST request is sent. The vulnerabilities could allow a remote user to send specially crafted queries to an authenticated user and steal their session cookie details, via the "/insert/source" petition, "name" parameter.	N/A	More Details
CVE-2025-53508	Multiple products provided by iND Co.,Ltd contain an OS command injection vulnerability. If exploited, an arbitrary OS command may be executed and sensitive information may be obtained. As for the details of affected product names and versions, refer to the information under [Product Status].	N/A	More Details
CVE-2025-58127	Improper Certificate Validation in Checkmk Exchange plugin Dell Powerscale allows attackers in MitM position to intercept traffic.	N/A	More Details
CVE-2025-30056	The RunCommand function accepts any parameter, which is then passed for execution in the shell. This allows an attacker to execute arbitrary code on the system.	N/A	More Details
CVE-2025-54544	QuickCMS is vulnerable to Stored XSS via aDirFilesDescriptions parameter in files editor functionality. Malicious attacker with admin privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting edited page. By default admin user is not able to add JavaScript into the website. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-34159	Coolify versions prior to v4.0.0-beta.420.6 are vulnerable to a remote code execution vulnerability in the application deployment workflow. The platform allows authenticated users, with low-level member privileges, to inject arbitrary Docker Compose directives during project creation. By crafting a malicious service definition that mounts the host root filesystem, an attacker can gain full root access to the underlying server.	N/A	More Details

CVE-2025-34161	Coolify versions prior to v4.0.0-beta.420.7 are vulnerable to a remote code execution vulnerability in the project deployment workflow. The platform allows authenticated users, with low-level member privileges, to inject arbitrary shell commands via the Git Repository field during project creation. By submitting a crafted repository string containing command injection syntax, an attacker can execute arbitrary commands on the underlying host system, resulting in full server compromise.	N/A	More Details
CVE-2025-50428	In RaspAP raspap-webgui 3.3.2 and earlier, a command injection vulnerability exists in the includes/hostapd.php script. The vulnerability is due to improper sanitizing of user input passed via the interface parameter.	N/A	More Details
CVE-2025-57845	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-34158. Reason: This candidate is a reservation duplicate of CVE-2025-34158. Notes: All CVE users should reference CVE-2025-34158 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-34523	A heap-based buffer overflow vulnerability exists in the exists in the network-facing input handling routines of Arcserve Unified Data Protection (UDP). This flaw is reachable without authentication and results from improper bounds checking when processing attacker-controlled input. By sending specially crafted data, a remote attacker can corrupt heap memory, potentially causing a denial of service or enabling arbitrary code execution depending on the memory layout and exploitation techniques used. This vulnerability is similar in nature to CVE-2025-34522 but affects a separate code path or component. No user interaction is required, and exploitation occurs in the context of the vulnerable process. This vulnerability affects all UDP versions prior to 10.2. UDP 10.2 includes the necessary patches and requires no action. Versions 8.0 through 10.1 are supported and require either patch application or upgrade to 10.2. Versions 7.x and earlier are unsupported or out of maintenance and must be upgraded to 10.2 to remediate the issue.	N/A	More Details
CVE-2025-34522	A heap-based buffer overflow vulnerability exists in the input parsing logic of Arcserve Unified Data Protection (UDP). This flaw can be triggered without authentication by sending specially crafted input to the target system. Improper bounds checking allows an attacker to overwrite heap memory, potentially leading to application crashes or remote code execution. Exploitation occurs in the context of the affected process and does not require user interaction. The vulnerability poses a high risk due to its pre-authentication nature and potential for full compromise. This vulnerability affects all UDP versions prior to 10.2. UDP 10.2 includes the necessary patches and requires no action. Versions 8.0 through 10.1 are supported and require either patch application or upgrade to 10.2. Versions 7.x and earlier are unsupported or out of maintenance and must be upgraded to 10.2 to remediate the issue.	N/A	More Details
	A reflected cross-site scripting (XSS) vulnerability exists in the web		

CVE-2025-34521	interface of the Arcserve Unified Data Protection (UDP), where unsanitized user input is improperly reflected in HTTP responses. This flaw allows remote attackers with low privileges to craft malicious links that, when visited by another user, execute arbitrary JavaScript in the victim's browser. Successful exploitation may lead to session hijacking, credential theft, or other client-side impacts. The vulnerability requires user interaction and occurs within a shared browser context. This vulnerability affects all UDP versions prior to 10.2. UDP 10.2 includes the necessary patches and requires no action. Versions 8.0 through 10.1 are supported and require either patch application or upgrade to 10.2. Versions 7.x and earlier are unsupported or out of maintenance and must be upgraded to 10.2 to remediate the issue.	N/A	More Details
CVE-2025-34520	An authentication bypass vulnerability in Arcserve Unified Data Protection (UDP) allows unauthenticated attackers to gain unauthorized access to protected functionality or user accounts. By manipulating specific request parameters or exploiting a logic flaw, an attacker can bypass login mechanisms without valid credentials and access administrator-level features. This vulnerability affects all UDP versions prior to 10.2. UDP 10.2 includes the necessary patches and requires no action. Versions 8.0 through 10.1 are supported and require either patch application or upgrade to 10.2. Versions 7.x and earlier are unsupported or out of maintenance and must be upgraded to 10.2 to remediate the issue.	N/A	More Details
CVE-2025-34163	Dongsheng Logistics Software exposes an unauthenticated endpoint at /CommMng/Print/UploadMailFile that fails to enforce proper file type validation and access control. An attacker can upload arbitrary files, including executable scripts such as .ashx, via a crafted multipart/form-data POST request. This allows remote code execution on the server, potentially leading to full system compromise. The vulnerability is presumed to affect builds released prior to July 2025 and is said to be remediated in newer versions of the product, though the exact affected range remains undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-07-23 UTC.	N/A	More Details
CVE-2025-34162	An unauthenticated SQL injection vulnerability exists in the GetLyfsByParams endpoint of Bian Que Feijiu Intelligent Emergency and Quality Control System, accessible via the /AppService/BQMedical/WebServiceForFirstaidApp.asmx interface. The backend fails to properly sanitize user-supplied input in the strOpid parameter, allowing attackers to inject arbitrary SQL statements. This can lead to data exfiltration, authentication bypass, and potentially remote code execution, depending on backend configuration. The vulnerability is presumed to affect builds released prior to June 2025 and is said to be remediated in newer versions of the product, though the exact affected range remains undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-07-23 UTC.	N/A	More Details
CVE-2025-57819	FreePBX is an open-source web-based graphical user interface. FreePBX 15, 16, and 17 endpoints are vulnerable due to insufficiently sanitized user-supplied data allowing unauthenticated access to FreePBX Administrator leading to arbitrary database manipulation and remote	N/A	More Details

	code execution. This issue has been patched in endpoint versions 15.0.66, 16.0.89, and 17.0.3.		
CVE-2025-34160	AnyShare contains a critical unauthenticated remote code execution vulnerability in the ServiceAgent API exposed on port 10250. The endpoint /api/ServiceAgent/start_service accepts user-supplied input via POST and fails to sanitize command-like payloads. An attacker can inject shell syntax that is interpreted by the backend, enabling arbitrary command execution. The vulnerability is presumed to affect builds released prior to August 2025 and is said to be remediated in newer versions of the product, though the exact affected range remains undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-07-11 UTC.	N/A	More Details
CVE-2024-13985	A command injection vulnerability in Dahua EIMS versions prior to 2240008 allows unauthenticated remote attackers to execute arbitrary system commands via the capture_handle.action interface. The flaw stems from improper input validation in the captureCommand parameter, which is processed without sanitization or authentication. By sending crafted HTTP requests, attackers can inject OS-level commands that are executed on the server, leading to full system compromise. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-04-06 UTC.	N/A	More Details
CVE-2024-13984	QiAnXin TianQing Management Center versions up to and including 6.7.0.4130 contain a path traversal vulnerability in the rptsvr component that allows unauthenticated attackers to upload files to arbitrary locations on the server. The /rptsvr/upload endpoint fails to sanitize the filename parameter in multipart form-data requests, enabling path traversal. This allows attackers to place executable files in web-accessible directories, potentially leading to remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-08-23 UTC.	N/A	More Details
CVE-2024-13982	SPON IP Network Broadcast System, a digital audio transmission platform developed by SPON Communications, contains an arbitrary file read vulnerability in the rj_get_token.php endpoint. The flaw arises from insufficient input validation on the jsondata[url] parameter, which allows attackers to perform directory traversal and access sensitive files on the server. An unauthenticated remote attacker can exploit this vulnerability by sending a crafted POST request to read arbitrary files, potentially exposing system configuration, credentials, or internal logic. An affected version range is undefined.	N/A	More Details
CVE-2024-13981	LiveBOS, an object-oriented business architecture middleware suite developed by Apex Software Co., Ltd., contains an arbitrary file upload vulnerability in its UploadFile.do;.js.jsp endpoint. This flaw affects the LiveBOS Server component and allows unauthenticated remote attackers to upload crafted files outside the intended directory structure via path traversal in the filename parameter. Successful exploitation may lead to remote code execution on the server, enabling full system compromise. The vulnerability is presumed to affect builds released prior to August 2024 and is said to be remediated in newer versions of	N/A	More Details

	the product, though the exact affected range remains undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-08-23 UTC.		
CVE-2025-58050	The PCRE2 library is a set of C functions that implement regular expression pattern matching. In version 10.45, a heap-buffer-overflow read vulnerability exists in the PCRE2 regular expression matching engine, specifically within the handling of the (*scs:...) (Scan SubString) verb when combined with (*ACCEPT) in src/pcre2_match.c. This vulnerability may potentially lead to information disclosure if the out-of-bounds data read during the memcmp affects the final match result in a way observable by the attacker. This issue has been resolved in version 10.46.	N/A	More Details
CVE-2024-13980	H3C Intelligent Management Center (IMC) versions up to and including E0632H07 contains a remote command execution vulnerability in the /byod/index.xhtml endpoint. Improper handling of JSF ViewState allows unauthenticated attackers to craft POST requests with forged javax.faces.ViewState parameters, potentially leading to arbitrary command execution. This flaw does not require authentication and may be exploited without session cookies. An affected version range is undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-08-28 UTC.	N/A	More Details
CVE-2024-13979	A SQL injection vulnerability exists in the St. Joe ERP system ("圣乔ERP系统") that allows unauthenticated remote attackers to execute arbitrary SQL commands via crafted HTTP POST requests to the login endpoint. The application fails to properly sanitize user-supplied input before incorporating it into SQL queries, enabling direct manipulation of the backend database. Successful exploitation may result in unauthorized data access, modification of records, or limited disruption of service. An affected version range is undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-04-14 UTC.	N/A	More Details
CVE-2024-13986	Nagios XI < 2024R1.3.2 contains a remote code execution vulnerability by chaining two flaws: an arbitrary file upload and a path traversal in the Core Config Snapshots interface. The issue arises from insufficient validation of file paths and extensions during MIB upload and snapshot rename operations. Exploitation results in the placement of attacker-controlled PHP files in a web-accessible directory, executed as the www-data user.	N/A	More Details
CVE-2025-58123	Improper Certificate Validation in Checkmk Exchange plugin BGP Monitoring allows attackers in MitM position to intercept traffic.	N/A	More Details
CVE-2018-25115	Multiple D-Link DIR-series routers, including DIR-110, DIR-412, DIR-600, DIR-610, DIR-615, DIR-645, and DIR-815 firmware version 1.03, contain a vulnerability in the service.cgi endpoint that allows remote attackers to execute arbitrary system commands without authentication. The flaw stems from improper input handling in the EVENT=CHECKFW parameter, which is passed directly to the system shell without sanitization. A crafted HTTP POST request can inject commands that are executed with root privileges, resulting in full device compromise.	N/A	More Details

	These router models are no longer supported at the time of assignment and affected version ranges may vary. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-08-21 UTC.		
CVE-2025-58124	Improper Certificate Validation in Checkmk Exchange plugin check-mk-api allows attackers in MitM position to intercept traffic.	N/A	More Details
CVE-2024-48908	lychee link checking action checks links in Markdown, HTML, and text files using lychee. Prior to version 2.0.2, there is a potential attack of arbitrary code injection vulnerability in lychee-setup of the composite action at action.yml. This issue has been patched in version 2.0.2.	N/A	More Details
CVE-2025-9578	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 40734.	N/A	More Details
CVE-2023-7307	Sangfor Behavior Management System (also referred to as DC Management System in Chinese-language documentation) contains an XML external entity (XXE) injection vulnerability in the /src/sangforindex endpoint. A remote unauthenticated attacker can submit crafted XML data containing external entity definitions, leading to potential disclosure of internal files, server-side request forgery (SSRF), or other impacts depending on parser behavior. The vulnerability is due to improper configuration of the XML parser, which allows resolution of external entities without restriction. This product is now integrated into their IAM (Internet Access Management) platform and an affected version range is undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-09-06 UTC.	N/A	More Details
CVE-2025-58125	Improper Certificate Validation in Checkmk Exchange plugin Freebox v6 agent allows attackers in MitM position to intercept traffic.	N/A	More Details
CVE-2023-7308	SecGate3600, a network firewall product developed by NSFOCUS, contains a sensitive information disclosure vulnerability in the /cgi-bin/authUser/authManageSet.cgi endpoint. The affected component fails to enforce authentication checks on POST requests to retrieve user data. An unauthenticated remote attacker can exploit this flaw to obtain sensitive information, including user identifiers and configuration details, by sending crafted requests to the vulnerable endpoint. An affected version range is undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-06-18 UTC.	N/A	More Details
CVE-2023-7309	A path traversal vulnerability exists in the Dahua Smart Park Integrated Management Platform (also referred to as the Dahua Smart Campus Integrated Management Platform), affecting the SOAP-based GIS bitmap upload interface. The flaw allows unauthenticated remote attackers to upload arbitrary files to the server via crafted SOAP requests, including executable JSP payloads. Successful exploitation may lead to remote code execution (RCE) and full compromise of the affected system. The vulnerability is presumed to affect builds released prior to September 2023 and is said to be remediated in newer versions of the product,	N/A	More Details

	though the exact affected range remains undefined. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-02-15 UTC.		
CVE-2025-34157	Coolify versions prior to v4.0.0-beta.420.6 are vulnerable to a stored cross-site scripting (XSS) attack in the project creation workflow. An authenticated user with low privileges can create a project with a maliciously crafted name containing embedded JavaScript. When an administrator attempts to delete the project or its associated resource, the payload executes in the admin’s browser context. This results in full compromise of the Coolify instance, including theft of API tokens, session cookies, and access to WebSocket-based terminal sessions on managed servers.	N/A	More Details
CVE-2025-46409	Inadequate encryption strength issue exists in SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier). If this vulnerability is exploited, a function that requires authentication may be accessed by a remote unauthenticated attacker.	N/A	More Details
CVE-2025-58062	LSTM-Kirigaya's openmcp-client is a vscode plugin for mcp developer. Prior to version 0.1.12, when users on a Windows platform connect to an attacker controlled MCP server, attackers could provision a malicious authorization server endpoint to silently achieve an OS command injection attack in the open() invocation, leading to client system compromise. This issue has been patched in version 0.1.12.	N/A	More Details
CVE-2025-58326	Rejected reason: Not used	N/A	More Details
CVE-2025-30057	In UHCRTFDoc, the filename parameter can be exploited to execute arbitrary code via command injection into the system() call in the ConvertToPDF function.	N/A	More Details
CVE-2025-30058	In the PatientService.pl service, the "getPatientIdentifier" function is vulnerable to SQL injection through the "pesel" parameter.	N/A	More Details
CVE-2025-30059	In the PrepareCDExportJSON.pl service, the "getPerfServiceIds" function is vulnerable to SQL injection.	N/A	More Details
CVE-2025-30060	In the ReturnUserUnitsXML.pl service, the "getUserInfo" function is vulnerable to SQL injection through the "UserID" parameter.	N/A	More Details
CVE-2025-30061	In the "utils/Reporter/OpenReportWindow.pl" service, there is an SQL injection vulnerability through the "UserID" parameter.	N/A	More Details
CVE-2025-30063	The configuration file containing database logins and passwords is readable by any local user.	N/A	More Details

CVE-2025-58333	Rejected reason: Not used	N/A	More Details
CVE-2025-58332	Rejected reason: Not used	N/A	More Details
CVE-2025-58331	Rejected reason: Not used	N/A	More Details
CVE-2025-58330	Rejected reason: Not used	N/A	More Details
CVE-2025-58329	Rejected reason: Not used	N/A	More Details
CVE-2025-58328	Rejected reason: Not used	N/A	More Details
CVE-2025-58327	Rejected reason: Not used	N/A	More Details
CVE-2025-58126	Improper Certificate Validation in Checkmk Exchange plugin VMware vSAN allows attackers in MitM position to intercept traffic.	N/A	More Details
CVE-2025-52460	Files or directories accessible to external parties issue exists in SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier). If exploited, uploaded files and SS1 configuration files may be accessed by a remote unauthenticated attacker.	N/A	More Details
CVE-2025-54543	QuickCMS is vulnerable to Stored XSS via sDescriptionMeta parameter in page editor SEO functionality. Malicious attacker with admin privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting edited page. By default admin user is not able to add JavaScript into the website. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-54542	QuickCMS sends password and login via GET Request. This allows a local attacker with access to the victim's browser history to obtain the necessary credentials to log in as the user. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details

CVE-2025-54541	QuickCMS is vulnerable to Cross-Site Request Forgery in page deletion functionality. Malicious attacker can craft special website, which when visited by the admin, will automatically send a POST request deleting an article. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-54540	QuickCMS is vulnerable to Reflected XSS via sSort parameter in admin's panel functionality. A malicious attacker can craft a specially crafted URL that, when opened, results in arbitrary JavaScript execution in the victim's browser. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-48963	Local privilege escalation due to improper soft link handling. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 40296.	N/A	More Details
CVE-2024-58240	In the Linux kernel, the following vulnerability has been resolved: tls: separate no-async decryption request handling from async If we're not doing async, the handling is much simpler. There's no reference counting, we just need to wait for the completion to wake us up and return its result. We should preferably also use a separate crypto_wait. I'm not seeing a UAF as I did in the past, I think aec7961916f3 ("tls: fix race between async notify and socket close") took care of it. This will make the next fix easier.	N/A	More Details
CVE-2025-58081	Use of hard-coded password issue/vulnerability in SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier) allows a remote unauthenticated attacker to view arbitrary files with root privileges.	N/A	More Details
CVE-2025-58072	Improper limitation of a pathname to a restricted directory ('Path Traversal') issue exists in SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier). If this vulnerability is exploited, arbitrary files may be viewed by a remote unauthenticated attacker.	N/A	More Details
CVE-2025-54819	Improper limitation of a pathname to a restricted directory ('Path Traversal') issue exists in SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier). If this vulnerability is exploited, legitimate files may be overwritten by a remote authenticated attacker.	N/A	More Details
CVE-2025-54762	SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier) allows a remote unauthenticated attacker to upload arbitrary files and execute OS commands with SYSTEM privileges.	N/A	More Details
CVE-2025-53970	SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier) allows a remote unauthenticated attacker to upload arbitrary files and execute OS commands with SYSTEM privileges.	N/A	More Details
CVE-2025-	Incorrect permission assignment for critical resource issue exists in SS1 Ver.16.0.0.10 and earlier (Media version:16.0.0a and earlier), which	N/A	More

53396	may allow users who can log in to a client terminal to obtain root privileges.		Details
CVE-2025-20296	A vulnerability in the web-based management interface of Cisco UCS Manager Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious data into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must be a member of the Administrator or AAA Administrator role.	N/A	More Details
CVE-2025-30064	An insufficiently secured internal function allows session generation for arbitrary users. The decodeParam function checks the JWT but does not verify which signing algorithm was used. As a result, an attacker can use the "ex:action" parameter in the VerifyUserByThrustedService function to generate a session for any user.	N/A	More Details