SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 October 2025

Generated on 15 October 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-2025-61913	Flowise is a drag & drop user interface to build a customized large language model flow. In versions prior to 3.0.8, WriteFileTool and ReadFileTool in Flowise do not restrict file path access, allowing authenticated attackers to exploit this vulnerability to read and write arbitrary files to any path in the file system, potentially leading to remote command execution. Flowise 3.0.8 fixes this vulnerability.	9.9	More Details
CVE-2025-49708	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2025-11539	Grafana Image Renderer is vulnerable to remote code execution due to an arbitrary file write vulnerability. This is due to the fact that the /render/csv endpoint lacked validation of the filePath parameter that allowed an attacker to save a shared object to an arbitrary location that is then loaded by the Chromium process. Instances are vulnerable if: 1. The default token ("authToken") is not changed, or is known to the attacker. 2. The attacker can reach the image renderer endpoint. This issue affects grafana-image-renderer: from 1.0.0 through 4.0.16.	9.9	More Details
CVE-2025-60306	code-projects Simple Car Rental System 1.0 has a permission bypass issue where low privilege users can forge high privilege sessions and perform sensitive operations.	9.9	More Details
CVE-2025-55315	Inconsistent interpretation of http requests ('http request/response smuggling') in ASP.NET Core allows an authorized attacker to bypass a security feature over a network.	9.9	More Details
CVE-2025-	A security vulnerability has been detected in Tenda CH22 up to 1.0.0.1. This issue affects the function formWrlsafeset of the file /goform/AdvSetWrlsafeset of the component HTTP Request Handler. The manipulation of the argument mit_ssid_index leads to stack-based buffer	9.8	More

11418	overflow. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.		Details
CVE-2025-59246	Azure Entra ID Elevation of Privilege Vulnerability	9.8	More Details
CVE-2025-42937	SAP Print Service (SAPSprint) performs insufficient validation of path information provided by users. An unauthenticated attacker could traverse to the parent directory and over-write system files causing high impact on confidentiality integrity and availability of the application.	9.8	More Details
CVE-2025-40771	A vulnerability has been identified in SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.4.24), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.4.24), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.4.24). Affected devices do not properly authenticate configuration connections. This could allow an unauthenticated remote attacker to access the configuration data.	9.8	More Details
CVE-2025-10610	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SFS Consulting Information Processing Industry and Foreign Trade Inc. Winsure allows Blind SQL Injection.This issue affects Winsure: through Version dated 21.08.2025.	9.8	More Details
CVE-2025-6919	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cats Information Technology Software Development Technologies Aykome License Tracking System allows SQL Injection.This issue affects Aykome License Tracking System: before Version dated 06.10.2025.	9.8	More Details
CVE-2025-6439	The WooCommerce Designer Pro plugin for WordPress, used by the Pricom - Printing Company & Design Services WordPress theme, is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'wcdp_save_canvas_design_ajax' function in all versions up to, and including, 1.9.26. This makes it possible for unauthenticated attackers to delete all files in an arbitrary directory on the server, which can lead to remote code execution, data loss, or site unavailability.	9.8	More Details
CVE-2025-6553	The Ovatheme Events Manager plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the process_checkout() function in all versions up to, and including, 1.8.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-11533	The WP Freeio plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.21. This is due to the process_register() function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2025-11423	A vulnerability was found in Tenda CH22 1.0.0.1. This affects the function formSafeEmailFilter of the file /goform/SafeEmailFilter. Performing manipulation of the argument page results in memory corruption. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2025-35051	Newforma Project Center Server (NPCS) accepts serialized .NET data via the '/ProjectCenter.rem' endpoint on 9003/tcp, allowing a remote, unauthenticated attacker to execute arbitrary code with 'NT AUTHORITY\NetworkService' privileges. According to the recommended architecture, the vulnerable NPCS endpoint is only accessible on an internal network. To mitigate this vulnerability, restrict network access to NPCS.	9.8	More Details
CVE-2025-40765	A vulnerability has been identified in TeleControl Server Basic V3.1 (All versions >= V3.1.2.2 < V3.1.2.3). The affected application contains an information disclosure vulnerability. This could allow an unauthenticated remote attacker to obtain password hashes of users and to login to and perform authenticated operations of the database service.	9.8	More Details
	Newforma Info Exchange (NIX) accepts serialized .NET data via the '/remoteweb/remote.rem'		

CVE-2025-35050	endpoint, allowing a remote, unauthenticated attacker to execute arbitrary code with 'NT AUTHORITY\NetworkService' privileges. The vulnerable endpoint is used by Newforma Project Center Server (NPCS), so a compromised NIX system can be used to attack an associated NPCS system. To mitigate this vulnerability, restrict network access to the '/remoteweb/remote.rem' endpoint, for example using the IIS URL Rewrite Module.	9.8	More Details
CVE-2025-59287	Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2025-11522	The Search & Go - Directory WordPress Theme theme for WordPress is vulnerable to Authentication Bypass via account takeover in all versions up to, and including, 2.7. This is due to insufficient user validation in the search_and_go_elated_check_facebook_user() function This makes it possible for unauthenticated attackers to gain access to other user's accounts, including administrators, when Facebook login is enabled.	9.8	More Details
CVE-2025-7634	The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 6.6.7 via the mode parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	9.8	More Details
CVE-2025-7526	The WP Travel Engine – Tour Booking Plugin – Tour Operator Software plugin for WordPress is vulnerable to arbitrary file deletion (via renaming) due to insufficient file path validation in the set_user_profile_image function in all versions up to, and including, 6.6.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.8	More Details
CVE-2025-10586	The Community Events plugin for WordPress is vulnerable to SQL Injection via the ‘event_venue’ parameter in all versions up to, and including, 1.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2025-10587	The Community Events plugin for WordPress is vulnerable to SQL Injection via the event_category parameter in all versions up to, and including, 1.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2025-46581	ZTE's ZXCDN product is affected by a Struts remote code execution (RCE) vulnerability. An unauthenticated attacker can remotely execute commands with non-root privileges.	9.8	More Details
CVE-2025-59218	Azure Entra ID Elevation of Privilege Vulnerability	9.6	More Details
CVE-2025-61929	Cherry Studio is a desktop client that supports for multiple LLM providers. Cherry Studio registers a custom protocol called `cherrystudio://`. When handling the MCP installation URL, it parses the base64-encoded configuration data and directly executes the command within it. In the files `src/main/services/ProtocolClient.ts` and `src/main/services/urlschema/mcp-install.ts`, when receiving a URL of the `cherrystudio://mcp` type, the `handleMcpProtocolUrl` function is called for processing. If an attacker crafts malicious content and posts it on a website or elsewhere (there are many exploitation methods, such as creating a malicious website with a button containing this malicious content), when the user clicks it, since the pop-up window contains normal content, the direct click is considered a scene action, and the malicious command is directly triggered, leading to the user being compromised. As of time of publication, no known patched versions exist.	9.6	More Details
CVE-2025-	BBOT's unarchive module could be abused by supplying malicious archives files and when extracted can then perform an arbitrary file write, resulting in remote code execution.	9.6	More Details

10284			
CVE-2025-10283	BBOT's gitdumper module could be abused to execute commands through a malicious git repository.	9.6	More Details
CVE-2025-56683	A cross-site scripting (XSS) vulnerability in the component /app/marketplace.html of Logseq v0.10.9 allows attackers to execute arbitrary code via injecting arbitrary Javascript into a crafted README.md file.	9.6	More Details
CVE-2025-60269	JEEWMS 20250820 is vulnerable to SQL Injection in the exportXls function located in the src/main/java/org/jeecgframework/web/cgreport/controller/excel/CgExportExcelController.java file.	9.4	More Details
CVE-2025-60316	SourceCodester Pet Grooming Management Software 1.0 is vulnerable to SQL Injection in admin/view_customer.php via the ID parameter.	9.4	More Details
CVE-2025-49553	Adobe Connect versions 12.9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute malicious scripts in a victim's browser. Exploitation of this issue requires user interaction in that a victim must navigate to a crafted web page. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Scope is changed.	9.3	More Details
CVE-2025-37729	Improper neutralization of special elements used in a template engine in Elastic Cloud Enterprise (ECE) can lead to a malicious actor with Admin access exfiltrating sensitive information and issuing commands via a specially crafted string where Jinjava variables are evaluated.	9.1	More Details
CVE-2025-42910	Due to missing verification of file type or content, SAP Supplier Relationship Management allows an authenticated attacker to upload arbitrary files. These files could include executables which might be downloaded and executed by the user which could host malware. On successful exploitation an attacker could cause high impact on confidentiality, integrity and availability of the application.	9.0	More Details
CVE-2025-9976	An OS Command Injection vulnerability affecting Station Launcher App in 3DEXPERIENCE platform from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2025x could allow an attacker to execute arbitrary code on the user's machine.	9.0	More Details
CVE-2025-59978	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to store script tags directly in web pages that, when viewed by another user, enable the attacker to execute commands with the target's administrative permissions. This issue affects all versions of Junos Space before 24.1R4.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-27059	Memory corruption while performing SCM call.	8.8	More Details
CVE-2025-40755	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP1). Affected applications are vulnerable to SQL injection through getTotalAndFilterCounts endpoint. An authenticated low privileged attacker could exploit to insert data and achieve privilege escalation. (ZDI-CAN-26570)	8.8	More Details
CVE-2025-58718	Use after free in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-	Improper authentication in Smart Switch prior to version 3.7.66.6 allows adjacent attackers to	8.8	More

21064	access transferring data.		Details
CVE-2025-8593	The GSheetConnector For Gravity Forms plugin for WordPress is vulnerable to authorization bypass in versions less than, or equal to, 1.3.27. This is due to a missing capability check on the 'install_plugin' function. This makes it possible for authenticated attackers, with subscriber-level access and above to install plugins on the target site and potentially achieve arbitrary code execution on the server under certain conditions.	8.8	More Details
CVE-2025-11561	A flaw was found in the integration of Active Directory and the System Security Services Daemon (SSSD) on Linux systems. In default configurations, the Kerberos local authentication plugin (sssd_krb5_localauth_plugin) is enabled, but a fallback to the an2ln plugin is possible. This fallback allows an attacker with permission to modify certain AD attributes (such as userPrincipalName or samAccountName) to impersonate privileged users, potentially resulting in unauthorized access or privilege escalation on domain-joined Linux hosts.	8.8	More Details
CVE-2025-9713	Path traversal in Ivanti Endpoint Manager allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	8.8	More Details
CVE-2025-59228	Improper input validation in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2025-11586	A vulnerability was determined in Tenda AC7 15.03.06.44. This affects an unknown function of the file /goform/setNotUpgrade. This manipulation of the argument newVersion causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2025-11549	A vulnerability has been found in Tenda W12 3.0.0.6(3948). The affected element is the function wifiMacFilterSet of the file /goform/modules of the component HTTP Request Handler. The manipulation of the argument mac leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-20710	In wlan AP driver, there is a possible out of bounds write due to an integer overflow. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00418785; Issue ID: MSV-3515.	8.8	More Details
CVE-2025-20720	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00418954; Issue ID: MSV-3569.	8.8	More Details
CVE-2025-20719	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00418955; Issue ID: MSV-3570.	8.8	More Details
CVE-2025-11444	A security vulnerability has been detected in TOTOLINK N600R up to 4.3.0cu.7866_B20220506. This impacts the function setWiFiBasicConfig of the file /cgi-bin/cstecgi.cgi of the component HTTP Request Handler. Such manipulation of the argument wepkey leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-20712	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00422323; Issue ID: MSV-3810.	8.8	More Details
CVE-2025-20711	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00422399; Issue ID: MSV-3748.	8.8	More Details

CVE-2025-41699	An low privileged remote attacker with an account for the Web-based management can change the system configuration to perform a command injection as root, resulting in a total loss of confidentiality, availability and integrity due to improper control of generation of code ('Code Injection').	8.8	More Details
CVE-2025-10228	Session Fixation vulnerability in Rolantis Information Technologies Agentis allows Session Hijacking.This issue affects Agentis: before 4.44.	8.8	More Details
CVE-2025-57457	An OS Command Injection vulnerability in the Admin panel in Curo UC300 5.42.1.7.1.63R1 allows local attackers to inject arbitrary OS Commands via the "IP Addr" parameter.	8.8	More Details
CVE-2025-59295	Heap-based buffer overflow in Internet Explorer allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-11653	A vulnerability was determined in UTT HiPER 2620G up to 3.1.4. Impacted is the function strcpy of the file /goform/fNTP. This manipulation of the argument NTPServerIP causes buffer overflow. It is possible to initiate the attack 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.	8.8	More Details
CVE-2025-10240	A vulnerability exists in the Progress Flowmon web application prior to version 12.5.5, whereby a user who clicks a malicious link provided by an attacker may inadvertently trigger unintended actions within their authenticated session.	8.8	More Details
CVE-2025-27060	Memory corruption while performing SCM call with malformed inputs.	8.8	More Details
CVE-2025-11528	A vulnerability was identified in Tenda AC7 15.03.06.44. This affects an unknown function of the file /goform/saveAutoQos. The manipulation of the argument enable leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-11527	A vulnerability was determined in Tenda AC7 15.03.06.44. The impacted element is an unknown function of the file /goform/fast_setting_pppoe_set. Executing manipulation of the argument Password can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2025-11526	A vulnerability was found in Tenda AC7 15.03.06.44. The affected element is an unknown function of the file /goform/WifiMacFilterSet. Performing manipulation of the argument wifi_chkHz results in stack-based buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2025-11525	A vulnerability has been found in Tenda AC7 15.03.06.44. Impacted is an unknown function of the file /goform/SetUpnpCfg. Such manipulation of the argument upnpEn leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-35055	Newforma Info Exchange (NIX) '/UserWeb/Common/UploadBlueimp.ashx' allows an authenticated attacker to upload an arbitrary file to any location writable by the NIX application. An attacker can upload and run a web shell or other content executable by the web server. An attacker can also delete directories. In Newforma before 2023.1, anonymous access is enabled by default (CVE-2025-35062), allowing an otherwise unauthenticated attacker to effectively authenticate as 'anonymous' and exploit this file upload vulnerability.	8.8	More Details
CVE-2025-11524	A flaw has been found in Tenda AC7 15.03.06.44. This issue affects some unknown processing of the file /goform/SetDDNSCfg. This manipulation of the argument ddnsEn causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-	The Lisfinity Core - Lisfinity Core plugin used for pebas® Lisfinity WordPress theme plugin for WordPress is vulnerable to privilege escalation via password update in all versions up to, and including, 1.4.0. This is due to the plugin not properly validating a user's identity prior to		More

2025-6038	updating their password. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary user's passwords, including those of administrators.	8.8	Details
CVE-2025-59249	Weak authentication in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2025-59237	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2025-58715	Integer overflow or wraparound in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	8.8	More Details
CVE-2025-58716	Improper input validation in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	8.8	More Details
CVE-2025-11651	A vulnerability has been found in UTT 进取 518G up to V3v3.2.7-210919-161313. This vulnerability affects the function sub_4247AC of the file /goform/formRemoteControl. The manipulation of the argument Profile leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-11652	A vulnerability was found in UTT 进取 518G up to V3v3.2.7-210919-161313. This issue affects some unknown processing of the file /goform/formTaskEdit_ap. The manipulation of the argument txtMin2 results in buffer overflow. The attack may be performed from remote. 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-2025-59247	Azure PlayFab Elevation of Privilege Vulnerability	8.8	More Details
CVE-2025-60311	ProjectWorlds Gym Management System1.0 is vulnerable to SQL Injection via the "id" parameter in the profile/edit.php page	8.8	More Details
CVE-2025-20709	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00415809; Issue ID: MSV-3405.	8.8	More Details
CVE-2025-25018	Improper Neutralization of Input During Web Page Generation in Kibana can lead to stored Cross-Site Scripting (XSS)	8.7	More Details
CVE-2025-10557	A stored Cross-site Scripting (XSS) vulnerability affecting Issue Management in ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-10558	A stored Cross-site Scripting (XSS) vulnerability affecting 3DSearch in 3DSwymer on Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-10556	A stored Cross-site Scripting (XSS) vulnerability affecting Specification Management in ENOVIA Specification Manager from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-55321	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Monitor allows an authorized attacker to perform spoofing over a network.	8.7	More Details

CVE-2025-59271	Redis Enterprise Elevation of Privilege Vulnerability	8.7	More Details
CVE-2025-10552	A stored Cross-site Scripting (XSS) vulnerability affecting 3DSwym in 3DSwymer on Release 3DEXPERIENCE R2025x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2025-59968	A Missing Authorization vulnerability in the Juniper Networks Junos Space Security Director allows an unauthenticated network-based attacker to read or modify metadata via the web interface. Tampering with this metadata can result in managed SRX Series devices permitting network traffic that should otherwise be blocked by policy, effectively bypassing intended security controls. This issue affects Junos Space Security Director * all versions prior to 24.1R3 Patch V4 This issue does not affect managed cSRX Series devices.	8.6	More Details
CVE-2025-61688	Omni manages Kubernetes on bare metal, virtual machines, or in a cloud. Prior to 1.1.5 and 1.0.2, Omni might leak sensitive information via an API.	8.6	More Details
CVE-2025-59889	Improper authentication of library files in the Eaton IPP software installer could lead to arbitrary code execution of an attacker with the access to the software package.	8.6	More Details
CVE-2025-48981	An insecure implementation of the proprietary protocol DNET in Product CGM MEDICO allows attackers within the intranet to eavesdrop and manipulate data on the protocol because encryption is optional for this connection.	8.6	More Details
CVE-2025-59146	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. An authenticated Server-Side Request Forgery (SSRF) vulnerability exists in versions prior to 0.9.0.5. A feature within the application allows authenticated users to submit a URL for the server to process its content. The application fails to properly validate this user-supplied URL before making a server-side request. This vulnerability is not limited to image URLs and can be triggered with any link provided to the vulnerable endpoint. Since user registration is often enabled by default, any registered user can exploit this. By crafting a malicious URL, an attacker can coerce the server to send requests to arbitrary internal or external services. The vulnerability has been patched in version 0.9.0.5. The patch introduces a comprehensive, user-configurable SSRF protection module, which is enabled by default to protect server security. This new feature provides administrators with granular control over outbound requests made by the server. For users who cannot upgrade immediately, some temporary mitigation options are available. Enable new-api image processing worker (new-api-worker) and/or configure egress firewall rules.	8.5	More Details
CVE-2025-59213	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Configuration Manager allows an unauthorized attacker to elevate privileges locally.	8.4	More Details
CVE-2025-23356	NVIDIA Isaac Lab contains a vulnerability in SB3 configuration parsing. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	8.4	More Details
CVE-2025-0636	EMCLI contains a high severity vulnerability where improper neutralization of special elements used in an OS command could be exploited leading to Arbitrary Code Execution.	8.4	More Details
CVE-2025-59974	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Junos Space Security Director allows an attacker to inject malicious scripts into the application, which are then stored and executed in the context of other users' browsers when they access affected pages.This issue affects Juniper Security Director: * All versions before 24.1R4.	8.4	More Details
CVE-2025-58299	Use After Free (UAF) vulnerability in the storage management module. Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-			

2025-59236	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2025-53782	Incorrect implementation of authentication algorithm in Microsoft Exchange Server allows an unauthorized attacker to elevate privileges locally.	8.4	More Details
CVE-2025-55903	A HTML injection vulnerability exists in Perfex CRM v3.3.1. The application fails to sanitize user input in the "Bill To" address field within the estimate module. As a result, arbitrary HTML can be injected and rendered unescaped in client-facing documents.	8.3	More Details
CVE-2025-60880	An authenticated stored XSS vulnerability exists in the Bagisto 2.3.6 admin panel's product creation path, allowing an attacker to upload a crafted SVG file containing malicious JavaScript code. This vulnerability can be exploited by an authenticated admin user to execute arbitrary JavaScript in the browser, potentially leading to session hijacking, data theft, or unauthorized actions.	8.3	More Details
CVE-2025-59292	External control of file name or path in Confidential Azure Container Instances allows an authorized attacker to elevate privileges locally.	8.2	More Details
CVE-2025-58325	An Incorrect Provision of Specified Functionality vulnerability [CWE-684] in FortiOS 7.6.0, 7.4.0 through 7.4.5, 7.2.5 through 7.2.10, 7.0.0 through 7.0.15, 6.4 all versions may allow a local authenticated attacker to execute system commands via crafted CLI commands.	8.2	More Details
CVE-2025-52650	Inline script execution allowed in CSP vulnerability has been identified in HCL AION v2.0	8.2	More Details
CVE-2025-23309	NVIDIA Display Driver contains a vulnerability where an uncontrolled DLL loading path might lead to arbitrary denial of service, escalation of privileges, code execution, and data tampering.	8.2	More Details
CVE-2025-59291	External control of file name or path in Confidential Azure Container Instances allows an authorized attacker to elevate privileges locally.	8.2	More Details
CVE-2025-25017	Improper Neutralization of Input During Web Page Generation in Kibana can lead to Cross-Site Scripting (XSS)	8.2	More Details
CVE-2025-54263	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Incorrect Authorization vulnerability. A low-privileged attacker could leverage this vulnerability to bypass security measures and maintain unauthorized access. Exploitation of this issue does not require user interaction.	8.1	More Details
CVE-2025-61930	Emlog is an open source website building system. Emlog Pro versions 2.5.19 and earlier are vulnerable to Cross-Site Request Forgery (CSRF) on the password change endpoint. An attacker can trick a logged-in administrator into submitting a crafted POST request to change the admin password without consent. Impact is account takeover of privileged users. Severity: High. As of time of publication, no known patched versions exist.	8.1	More Details
CVE-2025-54264	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by a stored Cross-Site Scripting (XSS) Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field. Scope is changed.	8.1	More Details
CVE-2025-	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Versions prior to 2.5.3 and 2.2.15 are vulnerable to Command Line Injection attacks on Windows when batch files are executed. In Windows, ``CreateProcess()`` always implicitly spawns ``cmd.exe`` if a batch file (.bat, .cmd, etc.) is being executed even if the application does not specify it via the command line.	8.1	More Details

61787	This makes Deno vulnerable to a command injection attack on Windows. Versions 2.5.3 and 2.2.15 fix the issue.		
CVE-2025-59250	Improper input validation in JDBC Driver for SQL Server allows an unauthorized attacker to perform spoofing over a network.	8.1	More Details
CVE-2025-36087	IBM Security Verify Access 10.0.0 through 10.0.9, 11.0.0, IBM Verify Identity Access Container 10.0.0 through 10.0.9, and 11.0.0, under certain configurations, contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	8.1	More Details
CVE-2025-61773	pyLoad is a free and open-source download manager written in Python. In versions prior to 0.5.0b3.dev91, pyLoad web interface contained insufficient input validation in both the Captcha script endpoint and the Click'N'Load (CNL) Blueprint. This flaw allowed untrusted user input to be processed unsafely, which could be exploited by an attacker to inject arbitrary content into the web UI or manipulate request handling. The vulnerability could lead to client-side code execution (XSS) or other unintended behaviors when a malicious payload is submitted. user-supplied parameters from HTTP requests were not adequately validated or sanitized before being passed into the application logic and response generation. This allowed crafted input to alter the expected execution flow. CNL (Click'N'Load) blueprint exposed unsafe handling of untrusted parameters in HTTP requests. The application did not consistently enforce input validation or encoding, making it possible for an attacker to craft malicious requests. Version 0.5.0b3.dev91 contains a patch for the issue.	8.1	More Details
CVE-2025-49201	A weak authentication in Fortinet FortiPAM 1.5.0, 1.4.0 through 1.4.2, 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager 7.2.0 through 7.2.4 allows attacker to execute unauthorized code or commands via specially crafted http requests	8.1	More Details
CVE-2025-62156	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Versions prior to 3.6.12 and versions 3.7.0 through 3.7.2 contain a Zip Slip path traversal vulnerability in artifact extraction. During artifact extraction the unpack/untar logic (workflow/executor/executor.go) uses filepath.Join(dest, filepath.Clean(header.Name)) without validating that header.Name stays within the intended extraction directory. A malicious archive entry can supply a traversal or absolute path that, after cleaning, overrides the destination directory and causes files to be written outside the /work/tmp extraction path and into system directories such as /etc inside the container. The vulnerability enables arbitrary file creation or overwrite in system configuration locations (for example /etc/passwd, /etc/hosts, /etc/crontab), which can lead to privilege escalation or persistence within the affected container. Update to 3.6.12 or 3.7.3 to remediate the issue.	8.1	More Details
CVE-2025-10494	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation when deleting profile pictures in all versions up to, and including, 1.4.89. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.1	More Details
CVE-2025-60378	Stored HTML injection in RISE Ultimate Project Manager & CRM allows authenticated users to inject arbitrary HTML into invoices and messages. Injected content renders in emails, PDFs, and messaging/chat modules sent to clients or team members, enabling phishing, credential theft, and business email compromise. Automated recurring invoices and messaging amplify the risk by distributing malicious content to multiple recipients.	8.1	More Details
CVE-2025-11695	When tlsInsecure=False appears in a connection string, certificate validation is disabled. This vulnerability affects MongoDB Rust Driver versions prior to v3.2.5	8.0	More Details
CVE-2025-53967	Framelink Figma MCP Server before 0.6.3 allows an unauthenticated remote attacker to execute arbitrary operating system commands via a crafted HTTP POST request with shell metacharacters in input that is used by a fetchWithRetry curl command. The vulnerable endpoint fails to properly sanitize user-supplied input, enabling the attacker to inject malicious commands that are executed with the privileges of the MCP process. Exploitation requires network access to the MCP interface.	8.0	More Details

CVE-2025-47355	Memory corruption while invoking remote procedure IOCTL calls.	7.8	More Details
CVE-2025-47347	Memory corruption while processing control commands in the virtual memory management interface.	7.8	More Details
CVE-2025-47338	Memory corruption while processing escape commands from userspace.	7.8	More Details
CVE-2025-47340	Memory corruption while processing IOCTL call to get the mapping.	7.8	More Details
CVE-2025-47341	memory corruption while processing an image encoding completion event.	7.8	More Details
CVE-2025-55328	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-47349	Memory corruption while processing an escape call.	7.8	More Details
CVE-2025-59275	Improper validation of specified type of input in Windows Authentication Methods allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-55692	Improper input validation in Windows Error Reporting allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59199	Improper access control in Software Protection Platform (SPP) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-47351	Memory corruption while processing user buffers.	7.8	More Details
CVE-2025-47354	Memory corruption while allocating buffers in DSP service.	7.8	More Details
CVE-2025-58287	Use After Free (UAF) vulnerability in the office service. Successful exploitation of this vulnerability may affect service confidentiality.	7.8	More Details
CVE-2025-55339	Out-of-bounds read in Windows NDIS allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59187	Improper input validation in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-53768	Use after free in Xbox allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-	Improper validation of specified type of input in Windows Authentication Methods allows an	7.8	More

59277	authorized attacker to elevate privileges locally.		Details
CVE-2025-27054	Memory corruption while processing a malformed license file during reboot.	7.8	More Details
CVE-2025-20713	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00432661; Issue ID: MSV-3904.	7.8	More Details
CVE-2025-20714	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00432659; Issue ID: MSV-3902.	7.8	More Details
CVE-2025-20715	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00421152; Issue ID: MSV-3731.	7.8	More Details
CVE-2025-20716	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00421149; Issue ID: MSV-3728.	7.8	More Details
CVE-2025-20717	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: WCNCR00419946; Issue ID: MSV-3582.	7.8	More Details
CVE-2025-20718	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00419945; Issue ID: MSV-3581.	7.8	More Details
CVE-2025-55696	Time-of-check time-of-use (toctou) race condition in NtQueryInformation Token function (ntifs.h) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-20721	In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10089545; Issue ID: MSV-4279.	7.8	More Details
CVE-2025-20723	In gnss driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09920033; Issue ID: MSV-3797.	7.8	More Details
CVE-2025-59191	Heap-based buffer overflow in Connected Devices Platform Service (Cdpsvc) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-55694	Improper access control in Windows Error Reporting allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59192	Buffer over-read in Storport.sys Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59494	Improper access control in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details

CVE-2025-59255	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59254	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59281	Improper link resolution before file access ('link following') in XBox Gaming Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-40809	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds write vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	7.8	More Details
CVE-2025-40810	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds write vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	7.8	More Details
CVE-2025-40811	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	7.8	More Details
CVE-2025-59290	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-40812	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	7.8	More Details
CVE-2025-59278	Improper validation of specified type of input in Windows Authentication Methods allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-53150	Use after free in Windows Digital Media allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59201	Improper access control in Network Connection Status Indicator (NCSI) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-55697	Heap-based buffer overflow in Azure Local allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-27048	Memory corruption while processing camera platform driver IOCTL calls.	7.8	More Details
CVE-2025-27053	Memory corruption during PlayReady APP usecase while processing TA commands.	7.8	More Details
CVE-2025-61862	An out-of-bounds read vulnerability exists in VS6ComFile!get_ovlp_element_size of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-	Use after free in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	7.8	More

59226			Details
CVE-2025-59227	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-54283	Illustrator versions 29.7, 28.7.9 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61859	An out-of-bounds write vulnerability exists in VS6ComFile!CItemDraw::is_motion_tween of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-61860	An out-of-bounds read vulnerability exists in VS6MemInIF!set_temp_type_default of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-61861	An out-of-bounds read vulnerability exists in VS6ComFile!load_link_inf of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-54282	Adobe Framemaker versions 2020.9, 2022.7 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-58722	Heap-based buffer overflow in Windows DWM allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-54281	Adobe Framemaker versions 2020.9, 2022.7 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61863	An out-of-bounds read vulnerability exists in VS6ComFile!CSaveData::delete_mem of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-54276	Substance3D - Modeler versions 1.22.3 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-58728	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-61864	A use after free vulnerability exists in VS6ComFile!load_link_inf of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-59230	Improper access control in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-58720	Use of a cryptographic primitive with a risky implementation in Windows Cryptographic Services allows an authorized attacker to disclose information locally.	7.8	More Details
CVE-2025-61807	Substance3D - Stager versions 3.1.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE-2025-59222	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-61856	A stack-based buffer overflow vulnerability exists in VS6ComFile!CV7BaseMap::WriteV7DataToRom of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-61803	Substance3D - Stager versions 3.1.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61805	Substance3D - Stager versions 3.1.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61802	Substance3D - Stager versions 3.1.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61801	Dimension versions 4.1.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61800	Dimension versions 4.1.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61857	An out-of-bounds write vulnerability exists in VS6ComFile!CItemExChange::WinFontDynStrCheck of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-59223	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-58724	Improper access control in Azure Connected Machine Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59224	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-61799	Dimension versions 4.1.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61806	Substance3D - Stager versions 3.1.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61798	Dimension versions 4.1.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a	7.8	More Details

	malicious file.		
CVE-2025-54284	Illustrator versions 29.7, 28.7.9 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-59225	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-59231	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-55680	Time-of-check time-of-use (toctou) race condition in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-24052	Microsoft is aware of vulnerabilities in the third party Agere Modem driver that ships natively with supported Windows operating systems. This is an announcement of the upcoming removal of ltmdm64.sys driver. The driver has been removed in the October cumulative update. Fax modem hardware dependent on this specific driver will no longer work on Windows. Microsoft recommends removing any existing dependencies on this hardware.	7.8	More Details
CVE-2025-55677	Untrusted pointer dereference in Windows Device Association Broker service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-62363	yt-grabber-tui is a terminal user interface application for downloading videos. In versions before 1.0-rc, the application allows users to configure the path to the yt-dlp executable via the path_to_yt_dlp configuration setting. An attacker with write access to the configuration file or the filesystem location of the configured executable can replace the executable with malicious code or create a symlink to an arbitrary executable. When the application invokes yt-dlp, the malicious code is executed with the privileges of the user running yt-grabber-tui. This vulnerability has been patched in version 1.0-rc.	7.8	More Details
CVE-2025-50175	Use after free in Windows Digital Media allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-50152	Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59243	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-55701	Improper validation of specified type of input in Microsoft Windows allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59242	Heap-based buffer overflow in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59241	Improper link resolution before file access ('link following') in Windows Health and Optimized Experiences Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59238	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-	Improper access control in Windows Ancillary Function Driver for WinSock allows an	7.8	More

58714	authorized attacker to elevate privileges locally.		Details
CVE-2025-59233	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-59207	Untrusted pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-11622	Insecure deserialization in Ivanti Endpoint Manager allows a local authenticated attacker to escalate their privileges.	7.8	More Details
CVE-2025-61858	An out-of-bounds write vulnerability exists in VS6ComFile!set_AnimationItem of V-SFT v6.2.7.0 and earlier. Opening specially crafted V-SFT files may lead to information disclosure, affected system's abnormal end (ABEND), and arbitrary code execution.	7.8	More Details
CVE-2025-59234	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-54280	Substance3D - Viewer versions 0.25.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-57741	An Incorrect Permission Assignment for Critical Resource vulnerability [CWE-732] in FortiClientMac 7.4.0 through 7.4.3, 7.2.0 through 7.2.11, 7.0 all versions may allow a local attacker to run arbitrary code or commands via LaunchDaemon hijacking.	7.8	More Details
CVE-2025-24990	Microsoft is aware of vulnerabilities in the third party Agere Modem driver that ships natively with supported Windows operating systems. This is an announcement of the upcoming removal of ltmdm64.sys driver. The driver has been removed in the October cumulative update. Fax modem hardware dependent on this specific driver will no longer work on Windows. Microsoft recommends removing any existing dependencies on this hardware.	7.8	More Details
CVE-2025-54274	Substance3D - Viewer versions 0.25.2 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-54273	Substance3D - Viewer versions 0.25.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-21062	Use of a broken or risky cryptographic algorithm in Smart Switch prior to version 3.7.67.2 allows local attackers to replace the restoring application. User interaction is required for triggering this vulnerability.	7.8	More Details
CVE-2025-10635	The Find Me On WordPress plugin through 2.0.9.1 does not sanitize and escape a parameter before using it in a SQL statement, allowing subscribers and above to perform SQL injection attacks	7.7	More Details
CVE-2025-11340	GitLab has remediated an issue in GitLab EE affecting all versions from 18.3 to 18.3.4, 18.4 to 18.4.2 that, under certain conditions, could have allowed authenticated users with read-only API tokens to perform unauthorized write operations on vulnerability records by exploiting incorrectly scoped GraphQL mutations.	7.7	More Details
CVE-2025-53139	Cleartext transmission of sensitive information in Windows Hello allows an unauthorized attacker to bypass a security feature locally.	7.7	More Details
CVE-2025-8459	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Monitoring recurrent downtime scheduler modules) allows Stored XSS.This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from	7.7	More Details

	24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.		
CVE-2025-55698	Null pointer dereference in Windows DirectX allows an authorized attacker to deny service over a network.	7.7	More Details
CVE-2025-59200	Concurrent execution using shared resource with improper synchronization ('race condition') in Data Sharing Service Client allows an unauthorized attacker to perform spoofing locally.	7.7	More Details
CVE-2025-33182	NVIDIA Jetson Linux contains a vulnerability in UEFI, where improper authentication may allow a privileged user to cause corruption of the Linux Device Tree. A successful exploitation of this vulnerability might lead to data tampering, denial of service.	7.6	More Details
CVE-2025-62162	cel-rust is a Common Expression Language interpreter written in Rust. Starting in version 0.10.0 and prior to version 0.11.4, parsing certain malformed CEL expressions can cause the parser to panic, terminating the process. When the crate is used to evaluate untrusted expressions (e.g., user-supplied input over an API), an attacker can send crafted input to trigger a denial of service (DoS). Version 0.11.4 fixes the issue.	7.5	More Details
CVE-2025-59530	quic-go is an implementation of the QUIC protocol in Go. In versions prior to 0.49.0, 0.54.1, and 0.55.0, a misbehaving or malicious server can cause a denial-of-service (DoS) attack on the quic-go client by triggering an assertion failure, leading to a process crash. This requires no authentication and can be exploited during the handshake phase. This was observed in the wild with certain server implementations. quic-go needs to be able to handle misbehaving server implementations, including those that prematurely send a HANDSHAKE_DONE frame. Versions 0.49.0, 0.54.1, and 0.55.0 discard Initial keys when receiving a HANDSHAKE_DONE frame, thereby correctly handling premature HANDSHAKE_DONE frames.	7.5	More Details
CVE-2025-60004	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial-Of-Service (DoS). When an affected system receives a specific BGP EVPN update message over an established BGP session, this causes an rpd crash and restart. A BGP EVPN configuration is not necessary to be vulnerable. If peers are not configured to send BGP EVPN updates to a vulnerable device, then this issue can't occur. This issue affects iBGP and eBGP, over IPv4 and IPv6. This issue affects: Junos OS: * 23.4 versions from 23.4R2-S3 before 23.4R2-S5, * 24.2 versions from 24.2R2 before 24.2R2-S1, * 24.4 versions before 24.4R1-S3, 24.4R2; Junos OS Evolved: * 23.4-EVO versions from 23.4R2-S2-EVO before 23.4R2-S5-EVO, * 24.2-EVO versions from 24.2R2-EVO before 24.2R2-S1-EVO, * 24.4-EVO versions before 24.4R1-S3-EVO, 24.4R2-EVO.	7.5	More Details
CVE-2025-25253	An Improper Validation of Certificate with Host Mismatch vulnerability [CWE-297] in FortiProxy version 7.6.1 and below, version 7.4.8 and below, 7.2 all versions, 7.0 all versions and FortiOS version 7.6.2 and below, version 7.4.8 and below, 7.2 all versions, 7.0 all versions ZTNA proxy may allow an unauthenticated attacker in a man-in-the middle position to intercept and tamper with connections to the ZTNA proxy	7.5	More Details
CVE-2025-41703	An unauthenticated remote attacker can cause a Denial of Service by turning off the output of the UPS via Modbus command.	7.5	More Details
CVE-2025-31717	In modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed.	7.5	More Details
CVE-2025-46774	An Improper Verification of Cryptographic Signature vulnerability [CWE-347] in FortiClient MacOS installer version 7.4.2 and below, version 7.2.9 and below, 7.0 all versions may allow a local user to escalate their privileges via FortiClient related executables.	7.5	More Details
CVE-2025-61601	BigBlueButton is an open-source virtual classroom. A Denial of Service (DoS) vulnerability in versions prior to 3.0.13 allows any authenticated user to freeze or crash the entire server by abusing the polling feature's `Choices` response type. By submitting a malicious payload with a massive array in the `answerIds` field, the attacker can cause the current meeting — and potentially all meetings on the server — to become unresponsive. Version 3.0.13 contains a patch. No known workarounds are available.	7.5	More Details

CVE-2025-9902	Authorization Bypass Through User-Controlled Key vulnerability in AKIN Software Computer Import Export Industry and Trade Co. Ltd. QRMenu allows Privilege Abuse.This issue affects QRMenu: from 1.05.12 before Version dated 05.09.2025.	7.5	More Details
CVE-2025-55326	Use after free in Connected Devices Platform Service (Cdpsvc) allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2025-61884	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: Runtime UI). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2025-57740	An Heap-based Buffer Overflow vulnerability [CWE-122] in FortiOS version 7.6.2 and below, version 7.4.7 and below, version 7.2.10 and below, 7.0 all versions, 6.4 all versions; FortiPAM version 1.5.0, version 1.4.2 and below, 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions and FortiProxy version 7.6.2 and below, version 7.4.3 and below, 7.2 all versions, 7.0 all versions RDP bookmark connection may allow an authenticated user to execute unauthorized code via crafted requests.	7.5	More Details
CVE-2025-11573	An infinite loop issue in Amazon.IonDotnet library versions <v1.3.2 may allow a threat actor to cause a denial of service through a specially crafted text input. To mitigate this issue, users should upgrade to version v1.3.2. As of August 20, 2025, this library has been deprecated and will not receive further updates.	7.5	More Details
CVE-2025-31718	In modem, there is a possible system crash due to improper input validation. This could lead to remote escalation of privilege with no additional execution privileges needed.	7.5	More Details
CVE-2025-61602	BigBlueButton is an open-source virtual classroom. A denial-of-service (DoS) vulnerability in versions prior to 3.0.13 allows any authenticated user to crash the chat functionality for all participants in a meeting by sending a malformed `reactionEmojiId` in the GraphQL mutation `chatSendMessageReaction`. Version 3.0.13 contains a patch. No known workarounds are available.	7.5	More Details
CVE-2025-61577	D-Link DIR-816A2_FWv1.10CNB05 was discovered to contain a stack overflow via the statuscheckpppoeuser parameter in the dir_setWanWifi function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-62170	rAthena is an open-source cross-platform MMORPG server. A use-after-free vulnerability exists in the RODEX functionality of rAthena's map-server in versions prior to commit af2f3ba. An unauthenticated attacker can exploit this vulnerability via a specific attacking scenario to cause a denial of service by crashing the map-server. This issue has been patched in commit af2f3ba. There are no known workarounds aside from manually applying the patch.	7.5	More Details
CVE-2025-59502	Uncontrolled resource consumption in Windows Remote Procedure Call allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2011-20001	A vulnerability has been identified in SIMATIC S7-1200 CPU V1 family (incl. SIPLUS variants) (All versions < V2.0.3), SIMATIC S7-1200 CPU V2 family (incl. SIPLUS variants) (All versions < V2.0.3). The web server interface of affected devices improperly processes incoming malformed HTTP traffic at high rate. This could allow an unauthenticated remote attacker to force the device entering the stop/defect state, thus creating a denial of service condition.	7.5	More Details
CVE-2025-41718	A cleartext transmission of sensitive information vulnerability in the affected products allows an unauthorized remote attacker to gain login credentials and access the Web-UI.	7.5	More Details
CVE-2025-58726	Improper access control in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details

CVE-2025-59248	Improper input validation in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2025-61920	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.5, Authlib's JOSE implementation accepts unbounded JWS/JWT header and signature segments. A remote attacker can craft a token whose base64url-encoded header or signature spans hundreds of megabytes. During verification, Authlib decodes and parses the full input before it is rejected, driving CPU and memory consumption to hostile levels and enabling denial of service. Version 1.6.5 patches the issue. Some temporary workarounds are available. Enforce input size limits before handing tokens to Authlib and/or use application-level throttling to reduce amplification risk.	7.5	More Details
CVE-2025-61919	Rack is a modular Ruby web server interface. Prior to versions 2.2.20, 3.1.18, and 3.2.3, `Rack::Request#POST` reads the entire request body into memory for `Content-Type: application/x-www-form-urlencoded`, calling `rack.input.read(nil)` without enforcing a length or cap. Large request bodies can therefore be buffered completely into process memory before parsing, leading to denial of service (DoS) through memory exhaustion. Users should upgrade to Rack version 2.2.20, 3.1.18, or 3.2.3, anu of which enforces form parameter limits using `query_parser.bytesize_limit`, preventing unbounded reads of `application/x-www-form-urlencoded` bodies. Additionally, enforce strict maximum body size at the proxy or web server layer (e.g., Nginx `client_max_body_size`, Apache `LimitRequestBody`).	7.5	More Details
CVE-2025-59975	An Uncontrolled Resource Consumption vulnerability in the HTTP daemon (httpd) of Juniper Networks Junos Space allows an unauthenticated network-based attacker flooding the device with inbound API calls to consume all resources on the system, leading to a Denial of Service (DoS). After continuously flooding the system with inbound connection requests, all available file handles become consumed, blocking access to the system via SSH and the web user interface (WebUI), resulting in a management interface DoS. A manual reboot of the system is required to restore functionality. This issue affects Junos Space: * all versions before 22.2R1 Patch V3, * from 23.1 before 23.1R1 Patch V3.	7.5	More Details
CVE-2025-11569	All versions of the package cross-zip are vulnerable to Directory Traversal via consecutive usage of zipSync() and unzipSync () functions that allow arguments such as __dirname. An attacker can access system files by selectively doing zip/unzip operations.	7.5	More Details
CVE-2025-10862	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Triggers plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 2.1.3. This is due to insufficient escaping on the 'id' parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-60536	An issue in the Configure New Cluster interface of kafka-ui v0.6.0 to v0.7.2 allows attackers to cause a Denial of Service (DoS) via uploading a crafted configuration file.	7.5	More Details
CVE-2025-59964	A Use of Uninitialized Resource vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX4700 devices allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When forwarding-options sampling is enabled, receipt of any traffic destined to the Routing Engine (RE) by the PFE line card leads to an FPC crash and restart, resulting in a Denial of Service (DoS). Continued receipt and processing of any traffic leading to the RE by the PFE line card will create a sustained Denial of Service (DoS) condition to the PFE line card. This issue affects Junos OS on SRX4700: * from 24.4 before 24.4R1-S3, 24.4R2 This issue affects IPv4 and IPv6.	7.5	More Details
CVE-2025-10004	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.12 to 18.2.8, 18.3 to 18.3.4, and 18.4 to 18.4.2 that could make the GitLab instance unresponsive or severely degraded by sending crafted GraphQL queries requesting large repository blobs.	7.5	More Details
CVE-2025-9970	Cleartext Storage of Sensitive Information in Memory vulnerability in ABB MConfig.This issue affects MConfig: through 1.4.9.21.	7.4	More Details

CVE-2024-33507	An insufficient session expiration vulnerability [CWE-613] and an incorrect authorization vulnerability [CWE-863] in FortiIsolator 2.4.0 through 2.4.4, 2.3 all versions, 2.2.0, 2.1 all versions, 2.0 all versions authentication mechanism may allow remote unauthenticated attacker to deauthenticate logged in admins via crafted cookie and remote authenticated read-only attacker to gain write privilege via crafted cookie.	7.4	More Details
CVE-2025-48004	Use after free in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2025-59206	Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability	7.4	More Details
CVE-2025-59210	Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability	7.4	More Details
CVE-2025-59189	Use after free in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2025-55687	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Resilient File System (ReFS) allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2025-11198	A Missing Authentication for Critical Function vulnerability in Juniper Networks Security Director Policy Enforcer allows an unauthenticated, network-based attacker to replace legitimate vSRX images with malicious ones. If a trusted user initiates deployment, Security Director Policy Enforcer will deliver the attacker's uploaded image to VMware NSX instead of a legitimate one. This issue affects Security Director Policy Enforcer: * All versions before 23.1R1 Hotpatch v3. This issue does not affect Junos Space Security Director Insights.	7.4	More Details
CVE-2025-55335	Use after free in Windows NTFS allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2025-40772	A vulnerability has been identified in SiPass integrated (All versions < V3.0). Affected server applications are vulnerable to stored Cross-Site Scripting (XSS), allowing an attacker to inject malicious code that can be executed by other users when they visit the affected page. Successful exploitation allows an attacker to impersonate other users within the application and steal their session data. This could enable unauthorized access to accounts and potentially lead to privilege escalation.	7.4	More Details
CVE-2025-55693	Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2011-20002	A vulnerability has been identified in SIMATIC S7-1200 CPU V1 family (incl. SIPLUS variants) (All versions < V2.0.2), SIMATIC S7-1200 CPU V2 family (incl. SIPLUS variants) (All versions < V2.0.2). Affected controllers are vulnerable to capture-replay in the communication with the engineering software. This could allow an on-path attacker between the engineering software and the controller to execute any previously recorded commands at a later time (e.g. set the controller to STOP), regardless whether or not the controller had a password configured.	7.4	More Details
CVE-2025-11584	A vulnerability has been found in code-projects Online Job Search Engine 1.0. The affected element is an unknown function of the file /searchjob.php. The manipulation of the argument txtspecialization leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-60375	The authentication mechanism in Perfex CRM before 3.3.1 allows attackers to bypass login credentials due to insufficient server-side validation. By sending empty username and password parameters in the login request, an attacker can gain unauthorized access to user accounts, including administrative accounts, without providing valid credentials.	7.3	More Details

CVE-2025-21058	Improper access control in Routines prior to version 4.8.7.1 in Android 15 and 4.9.6.0 in Android 16 allows local attackers to potentially execute arbitrary code with SystemUI privilege.	7.3	More Details
CVE-2025-11585	A vulnerability was found in code-projects Project Monitoring System 1.0. The impacted element is an unknown function of the file /useredit.php. The manipulation of the argument uid results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-11583	A flaw has been found in code-projects Online Job Search Engine 1.0. Impacted is an unknown function of the file /postjob.php. Executing manipulation of the argument txtjobID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-60869	Publii CMS v0.46.5 (build 17089) allows persistent Cross-Site Scripting (XSS) via unsanitized input in configuration fields such as "Site Description" and "Footer Follow Buttons". An attacker can inject arbitrary JavaScript, which is stored in the project and executed in the browsers of remote visitors viewing the generated static site.	7.3	More Details
CVE-2025-11188	The Kiwire Captive Portal contains a blind SQL injection in the nas-id parameter, allowing for SQL commands to be issued and to compromise the corresponding database.	7.3	More Details
CVE-2025-11189	The Kiwire Captive Portal contains a reflected cross-site scripting (XSS) vulnerability within the login-url parameter, allowing for Javascript execution.	7.3	More Details
CVE-2025-11582	A vulnerability was detected in code-projects Online Job Search Engine 1.0. This issue affects some unknown processing of the file /registration.php. Performing manipulation of the argument txtusername results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-30001	Incorrect Execution-Assigned Permissions vulnerability in Apache StreamPark. This issue affects Apache StreamPark: from 2.1.4 before 2.1.6. Users are recommended to upgrade to version 2.1.6, which fixes the issue.	7.3	More Details
CVE-2025-11557	A vulnerability has been found in projectworlds Gate Pass Management System 1.0. This issue affects some unknown processing of the file /add-pass.php. Such manipulation of the argument fullname leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11488	A weakness has been identified in D-Link DIR-852 up to 20251002. This affects an unknown part of the file /HNAP1/. Executing manipulation can lead to command injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2025-11596	A vulnerability was determined in code-projects E-Commerce Website 1.0. The affected element is an unknown function of the file /pages/delete_order_details.php. Executing manipulation of the argument order_id can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-11507	A weakness has been identified in PHPGurukul Beauty Parlour Management System 1.1. The impacted element is an unknown function of the file /admin/search-invoices.php. This manipulation of the argument searchdata causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-11506	A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. The affected element is an unknown function of the file /admin/search-appointment.php. The manipulation of the argument searchdata results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-	A vulnerability was identified in PHPGurukul Beauty Parlour Management System 1.1. Impacted is an unknown function of the file /admin/new-appointment.php. The manipulation of the argument delid leads to sql injection. It is possible to initiate the attack remotely. The	7.3	More Details

11505	exploit is publicly available and might be used.		
CVE-2025-11503	A vulnerability was determined in PHPGurukul Beauty Parlour Management System 1.1. This issue affects some unknown processing of the file /admin/manage-services.php. Executing manipulation of the argument delid can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-25004	Improper access control in Microsoft PowerShell allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2025-11558	A vulnerability was found in code-projects E-Commerce Website 1.0. Impacted is an unknown function of the file /pages/user_index_search.php. Performing manipulation of the argument Search 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-2025-11480	A vulnerability was detected in SourceCodester Simple E-Commerce Bookstore 1.0. The affected element is an unknown function of the file /register.php. Performing manipulation of the argument register_username results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-11479	A security vulnerability has been detected in SourceCodester Wedding Reservation Management System 1.0. Impacted is the function insertReservation of the file function.php. Such manipulation of the argument number leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-11599	A weakness has been identified in Campcodes Online Apartment Visitor Management System 1.0. This impacts an unknown function of the file /forgot-password.php. This manipulation of the argument email causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-11601	A vulnerability was detected in SourceCodester Online Student Result System 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. Performing manipulation of the argument Username results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-11477	A security flaw has been discovered in SourceCodester Wedding Reservation Management System 1.0. This vulnerability affects unknown code of the file /global.php. The manipulation of the argument User results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-11476	A vulnerability was identified in SourceCodester Simple E-Commerce Bookstore 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument login_username leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11475	A vulnerability was determined in projectworlds Advanced Library Management System 1.0. Affected by this issue is some unknown functionality of the file /view_member.php. Executing manipulation of the argument user_id can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-11604	A vulnerability was determined in projectworlds Online Ordering Food System 1.0. This issue affects some unknown processing of the file /all-orders.php. This manipulation of the argument Status causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-11473	A vulnerability has been found in SourceCodester Hotel and Lodge Management System 1.0. Affected is an unknown function of the file /edit_curr.php. Such manipulation of the argument currsymbol leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11472	A flaw has been found in SourceCodester Hotel and Lodge Management System 1.0. This impacts an unknown function of the file /edit_room.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been	7.3	More Details

	published and may be used.		
CVE-2025-11471	A vulnerability was detected in SourceCodester Hotel and Lodge Management System 1.0. This affects an unknown function of the file /edit_customer.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2025-11608	A security vulnerability has been detected in code-projects E-Banking System 1.0. This affects an unknown function of the file /register.php of the component POST Parameter Handler. The manipulation of the argument username/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-11434	A weakness has been identified in itsourcecode Student Transcript Processing System 1.0. Affected is an unknown function of the file /login.php. Executing manipulation of the argument uname can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-11614	A vulnerability was identified in SourceCodester Best Salon Management System 1.0. Affected by this issue is some unknown functionality of the file /panel/edit-appointment.php. Such manipulation of the argument editid leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11432	A vulnerability was identified in itsourcecode Leave Management System 1.0. This affects an unknown function of the file /reset.php. Such manipulation of the argument employid leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11430	A vulnerability was found in SourceCodester Simple E-Commerce Bookstore 1.0. The affected element is an unknown function of the file /cart.php. The manipulation of the argument remove results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-11424	A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. This impacts an unknown function of the file /login.php. Executing manipulation of the argument emailid can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-11422	A vulnerability has been found in Campcodes Advanced Online Voting Management System 1.0. The impacted element is an unknown function of the file /admin/login.php. Such manipulation of the argument Username leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11615	A security flaw has been discovered in SourceCodester Best Salon Management System 1.0. This affects an unknown part of the file /panel/add_invoice.php. Performing manipulation of the argument ServiceId results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-49552	Adobe Connect versions 12.9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a high-privileged attacker to execute malicious scripts in a victim's browser. Exploitation of this issue requires user interaction in that a victim must navigate to a crafted web page. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Scope is changed.	7.3	More Details
CVE-2025-11420	A vulnerability was detected in code-projects E-Commerce Website 1.0. Impacted is an unknown function of the file /pages/edit_order_details.php. The manipulation of the argument order_id results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-11513	A vulnerability was determined in code-projects E-Commerce Website 1.0. This affects an unknown part of the file /pages/supplier_update.php. This manipulation of the argument supp_id causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
	A security vulnerability has been detected in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This impacts an unknown		

CVE-2025-11657	function of the file /assets/createNotice.php. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available.	7.3	More Details
CVE-2025-11656	A weakness has been identified in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This affects an unknown function of the file /assets/editNotes.php. Executing manipulation of the argument File can lead to unrestricted upload. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	7.3	More Details
CVE-2025-11662	A security flaw has been discovered in SourceCodester Best Salon Management System 1.0. Impacted is an unknown function of the file /booking.php. The manipulation of the argument serv_id results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-11654	A vulnerability was identified in yousaf530 Inferno Online Clothing Store up to 827dd42bfbe380e8de76fdc67958c24cf1246208. The affected element is an unknown function of the file /log.php. Such manipulation of the argument cemail/password leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-45095	Lavasoft Web Companion (also known as Ad-Aware WebCompanion) versions 8.9.0.1091 through 12.1.3.1037 installs the DCIService.exe service with an unquoted service path vulnerability. An attacker with write access to the file system could potentially execute arbitrary code with elevated privileges by placing a malicious executable in the unquoted path.	7.3	More Details
CVE-2025-11529	A security flaw has been discovered in ChurchCRM up to 5.18.0. This impacts the function AuthMiddleware of the file src/ChurchCRM/Slim/Middleware/AuthMiddleware.php of the component API Endpoint. The manipulation results in missing authentication. The attack can be executed remotely. The exploit has been released to the public and may be exploited. The patch is identified as 3a1cffd2aea63d884025949cfbcfd274d06216a4. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2025-11736	A flaw has been found in itsourcecode Online Examination System 1.0. Affected by this issue is some unknown functionality of the file /index.php. This manipulation of the argument Username causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-57618	A path traversal vulnerability in FastX3 thru 3.3.67 allows an unauthenticated attacker to read arbitrary files on the server. By leveraging this vulnerability, it is possible to access the application's configuration files, which contain the secret key used to sign JSON Web Tokens as well as existing JTIs. With this information, an attacker can forge valid JWTs, impersonate the root user, and achieve remote code execution in privileged context via authenticated endpoints.	7.3	More Details
CVE-2025-11658	A vulnerability was detected in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. Affected is an unknown function of the file /assets/changeSllyabus.php. The manipulation of the argument File results in unrestricted upload. The attack may be launched remotely. The exploit is now public and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	7.3	More Details
CVE-2025-11659	A flaw has been found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. Affected by this vulnerability is an unknown functionality of the file /assets/uploadNotes.php. This manipulation of the argument File causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	7.3	More Details

CVE-2025-11661	A vulnerability was found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. This affects an unknown part. Performing manipulation results in missing authentication. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to maintain continuous delivery	7.3	More Details
CVE-2025-11660	A vulnerability has been found in ProjectsAndPrograms School Management System up to 6b6fae5426044f89c08d0dd101c7fa71f9042a59. Affected by this issue is some unknown functionality of the file /assets/uploadSllyabus.php. Such manipulation of the argument File leads to unrestricted upload. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable.	7.3	More Details
CVE-2025-55240	Improper access control in Visual Studio allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2025-55247	Improper link resolution before file access ('link following') in .NET allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2025-58298	Data processing error vulnerability in the package management module. Successful exploitation of this vulnerability may affect availability.	7.3	More Details
CVE-2025-11555	A vulnerability was detected in Campcodes Online Learning Management System 1.0. This affects an unknown part of the file /admin/calendar_of_events.php. The manipulation of the argument date_start results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-11556	A flaw has been found in code-projects Simple Leave Manager 1.0. This vulnerability affects unknown code of the file /user.php. This manipulation of the argument table causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	7.3	More Details
CVE-2025-60535	A Cross-Site Request Forgery (CSRF) in the component /endpoints/currency/currency of Wallos v4.1.1 allows attackers to execute arbitrary operations via a crafted GET request.	7.3	More Details
CVE-2024-50571	A heap-based buffer overflow in Fortinet FortiOS 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.10, 7.0.0 through 7.0.16, 6.4.0 through 6.4.15, 6.2.0 through 6.2.17, FortiManager Cloud 7.6.2, 7.4.1 through 7.4.5, 7.2.1 through 7.2.8, 7.0.1 through 7.0.13, 6.4.1 through 6.4.7, FortiAnalyzer Cloud 7.4.1 through 7.4.5, 7.2.1 through 7.2.8, 7.0.1 through 7.0.13, 6.4.1 through 6.4.7, FortiProxy 7.6.0, 7.4.0 through 7.4.6, 7.2.0 through 7.2.12, 7.0.0 through 7.0.19, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiAnalyzer 7.6.0 through 7.6.2, 7.4.0 through 7.4.5, 7.2.0 through 7.2.8, 7.0.0 through 7.0.13, 6.4.0 through 6.4.15, 6.2.0 through 6.2.13, 6.0.0 through 6.0.12, FortiManager 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.9, 7.0.0 through 7.0.13, 6.4.0 through 6.4.15, 6.2.0 through 6.2.13, 6.0.0 through 6.0.12 allows attacker to execute unauthorized code or commands via specifically crafted requests.	7.2	More Details
CVE-2025-10985	OS command injection in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2025-11675	Enterprise Cloud Database developed by Ragic has an Arbitrary File Upload vulnerability, allowing privileged remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2025-5946	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Centreon Infra Monitoring (Poller reload setup in the configuration modules) allows OS Command Injection. On the poller parameters page, a user with high privilege is able to concatenate custom instructions into the poller reload command. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from	7.2	More Details

	23.10.0 before 23.10.28.		
CVE-2025-11204	The RegistrationMagic – Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 6.0.6.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator access or higher, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. An unauthenticated attacker could utilize an injected Cross-Site Scripting via user-agent on form submission to leverage this to achieve Reflected Cross-Site Scripting.	7.2	More Details
CVE-2025-11673	SOOP-CLM developed by PiExtract has a Hidden Functionality vulnerability, allowing privileged remote attackers to exploit a hidden functionality to execute arbitrary code on the server.	7.2	More Details
CVE-2025-10239	In Flowmon versions prior to 12.5.5, a vulnerability has been identified that allows a user with administrator privileges and access to the management interface to execute additional unintended commands within scripts intended for troubleshooting purposes.	7.2	More Details
CVE-2025-10496	The Cookie Notice & Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the uuid parameter in all versions up to, and including, 1.6.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-37134	An authenticated command injection vulnerability exists in the CLI binary of an AOS-8 Controller/Mobility Conductor operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2025-37133	An authenticated command injection vulnerability exists in the CLI binary of an AOS-8 Controller/Mobility Conductor operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2025-10243	OS command injection in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2025-10242	OS command injection in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2025-37146	A vulnerability in the web-based management interface of network access point configuration services could allow an authenticated remote attacker to perform remote command execution. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.	7.2	More Details
CVE-2025-47856	Two improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiVoice version 7.2.0, 7.0.0 through 7.0.6 and before 6.4.10 allows a privileged attacker to execute arbitrary code or commands via crafted HTTP/HTTPS or CLI requests.	7.2	More Details
CVE-2025-61524	An issue in the permission verification module and organization/application editing interface in Casdoor v2.26.0 and before, and fixed in v.2.63.0, allows remote authenticated administrators of any organization within the system to bypass the system's permission verification mechanism by directly concatenating URLs after login	7.2	More Details
CVE-2025-37132	An arbitrary file write vulnerability exists in the web-based management interface of both the AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to upload arbitrary files and execute arbitrary commands on the underlying operating system.	7.2	More Details
CVE-	BigBlueButton is an open-source virtual classroom. In versions prior to 3.0.13, the "Shared Notes" feature contains a Stored Cross-Site Scripting (XSS) vulnerability with the input location		

2025-55200	being the "Username" field and the output location on the "Shared Notes" page, when a user with a malicious username is editing content. This vulnerability allows a low-privileged user to execute arbitrary JavaScript in the context of higher-privileged users (e.g., Admins) who open the Shared Notes page. Version 3.0.13 fixes the issue.	7.1	More Details
CVE-2025-47342	Transient DOS may occur when multi-profile concurrency arises with QHS enabled.	7.1	More Details
CVE-2025-21050	Improper input validiation in Contacts prior to SMR Oct-2025 Release 1 allows local attackers to access data across multiple user profiles.	7.1	More Details
CVE-2025-37147	A Secure Boot Bypass Vulnerability exists in affected Access Points that allows an adversary to bypass the hardware root of trust verification in place to ensure only vendor-signed firmware can execute on the device. An adversary can exploit this vulnerability to run modified or custom firmware on affected Access Points.	7.1	More Details
CVE-2025-21061	Cleartext storage of sensitive information in Smart Switch prior to version 3.7.67.2 allows local attackers to access sensitive data. User interaction is required for triggering this vulnerability.	7.1	More Details
CVE-2025-59235	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	7.1	More Details
CVE-2025-59208	Out-of-bounds read in Windows MapUrlToZone allows an unauthorized attacker to disclose information over a network.	7.1	More Details
CVE-2025-59232	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	7.1	More Details
CVE-2025-23280	NVIDIA Display Driver for Linux contains a vulnerability where an attacker could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.0	More Details
CVE-2025-58733	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-59195	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to deny service locally.	7.0	More Details
CVE-2025-59194	Use of uninitialized resource in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55689	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55690	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55691	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55688	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details

CVE-2025-58732	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-59202	Use after free in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-58735	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-23282	NVIDIA Display Driver for Linux contains a vulnerability where an attacker might be able to use a race condition to escalate privileges. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.0	More Details
CVE-2025-11649	A vulnerability was found in Tomofun Furbo 360 and Furbo Mini. The affected element is an unknown function of the component Root Account Handler. Performing manipulation results in use of hard-coded password. The attack must be initiated from a local position. The attack is considered to have high complexity. The exploitability is described as difficult. The exploit has been made public and could be used. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2025-59193	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59205	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-58736	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-58730	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-58734	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-58727	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-58738	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-58725	Heap-based buffer overflow in Windows COM allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-58737	Use after free in Windows Remote Desktop allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-59196	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-			

2025-58731	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-55686	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55681	Out-of-bounds read in Windows DWM allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59289	Double free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59497	Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Linux allows an authorized attacker to deny service locally.	7.0	More Details
CVE-2025-50174	Use after free in Windows Device Association Broker service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59282	Concurrent execution using shared resource with improper synchronization ('race condition') in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-47989	Improper access control in Azure Connected Machine Agent allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59261	Time-of-check time-of-use (toctou) race condition in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-53717	Reliance on untrusted inputs in a security decision in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55331	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55340	Improper authentication in Windows Remote Desktop Protocol allows an authorized attacker to bypass a security feature locally.	7.0	More Details
CVE-2025-55678	Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59285	Deserialization of untrusted data in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-55685	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2024-48891	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiSOAR 7.6.0 through 7.6.1, 7.5.0 through 7.5.1, 7.4 all versions, 7.3 all versions may allow an attacker who has already obtained a non-login low privileged shell access (via another hypothetical vulnerability) to perform a local privilege escalation via crafted commands.	7.0	More Details

CVE-2025-59221	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2025-55684	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-54889	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (SNMP traps manufacturer configuration modules) allows Stored XSS by users with elevated privileges. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-9698	The Plus Addons for Elementor WordPress plugin before 6.3.16 does not sanitize SVG file contents, which could allow users with minimum role access as Author to perform Stored Cross-Site Scripting attacks.	6.8	More Details
CVE-2025-54891	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (ACL Resource access configuration modules) allows Stored XSS by users with elevated privileges. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-9975	The WP Scraper plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.8.1 via the wp_scraper_extract_content function. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. On Cloud instances, this issue allows for metadata retrieving.	6.8	More Details
CVE-2025-54893	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Hosts templates configuration modules) allows Stored XSS by users with elevated privileges. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-41705	An unauthenticated remote attacker (MITM) can intercept the websocket messages to gain access to the login credentials for the Webfrontend.	6.8	More Details
CVE-2025-54892	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (SNMP traps group configuration modules) allows Stored XSS by users with elevated privileges. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-8429	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (ACL Action access configuration modules) allows Stored XSS by users with elevated privileges. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-11674	SOOP-CLM developed by PiExtract has a Server-Side Request Forgery vulnerability, allowing privileged remote attackers to read server files or probe internal network information.	6.8	More Details
CVE-2025-8430	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Commands Connectors configuration modules) allows Stored XSS by users with elevated privileges. This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-	An Origin Validation Error vulnerability in an insufficient protected file of Juniper Networks Junos OS on EX4600 Series and QFX5000 Series allows an unauthenticated attacker with physical access to the device to create a backdoor which allows complete control of the system. When a device isn't configured with a root password, an attacker can modify a specific file. It's contents will be added to the Junos configuration of the device without being visible. This allows for the addition of any configuration unknown to the actual operator, which includes users, IP addresses and other configuration which could allow unauthorized access to the device. This exploit is persistent across reboots and even zeroization. The indicator of	6.8	More Details

59957	compromise is a modified /etc/config/<platform>-defaults[-flex].conf file. Review that file for unexpected configuration statements, or compare it to an unmodified version which can be extracted from the original Juniper software image file. For details on the extraction procedure please contact Juniper Technical Assistance Center (JTAC). To restore the device to a trusted initial configuration the system needs to be reinstalled from physical media. This issue affects Junos OS on EX4600 Series and QFX5000 Series: * All versions before 21.4R3, * 22.2 versions before 22.2R3-S3.		
CVE-2025-8428	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (HTTP Loader widget modules) allows Stored XSS.This issue affects Infra Monitoring: from 24.10.0 before 24.10.13, from 24.04.0 before 24.04.18, from 23.10.0 before 23.10.28.	6.8	More Details
CVE-2025-57716	An Uncontrolled Search Path Element vulnerability [CWE-427] in FortiClient Windows 7.4.0 through 7.4.3, 7.2.0 through 7.2.11, 7.0 all versions may allow a local low privileged user to perform a DLL hijacking attack via placing a malicious DLL to the FortiClient Online Installer installation folder.	6.7	More Details
CVE-2025-11666	A flaw has been found in Tenda RP3 Pro up to 22.5.7.93. This impacts an unknown function of the file force_upgrade.sh of the component Firmware Update Handler. Executing manipulation of the argument current_force_upgrade_pwd can lead to use of hard-coded password. The attack can only be executed locally. The exploit has been published and may be used.	6.7	More Details
CVE-2025-55320	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Configuration Manager allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-8886	Incorrect Permission Assignment for Critical Resource, Exposure of Sensitive Information to an Unauthorized Actor, Missing Authorization, Incorrect Authorization vulnerability in Usta Information Systems Inc. Aybs Interaktif allows Privilege Abuse, Authentication Bypass.This issue affects Aybs Interaktif: from 2024 through 28082025.	6.7	More Details
CVE-2023-46718	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.	6.7	More Details
CVE-2025-21048	Relative path traversal in Knox Enterprise prior to SMR Oct-2025 Release 1 allows local attackers to execute arbitrary code.	6.7	More Details
CVE-2025-27039	Memory corruption may occur while processing IOCTL call for DMM/WARPNCC CONFIG request.	6.6	More Details
CVE-2025-21065	Improper input validation in Retail Mode prior to version 5.59.11 allows self attackers to execute privileged commands on their own devices.	6.6	More Details
CVE-2025-27040	Information disclosure may occur while processing the hypervisor log.	6.5	More Details
CVE-2025-53845	An improper authentication vulnerability [CWE-287] in Fortinet FortiAnalyzer version 7.6.0 through 7.6.3 and before 7.4.6 allows an unauthenticated attacker to obtain information pertaining to the device's health and status, or cause a denial of service via crafted OFTP requests.	6.5	More Details
CVE-2025-10649	The Welcart e-Commerce plugin for WordPress is vulnerable to SQL Injection via the cookie in all versions up to, and including, 2.11.21 due to insufficient escaping on the user supplied value and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details

CVE-2025-10249	The Slider Revolution plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on several functions in all versions up to, and including, 6.7.37. This makes it possible for authenticated attackers, with Contributor-level access and above, to install and activate plugin add-ons, create sliders, and download arbitrary files.	6.5	More Details
CVE-2025-59921	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiADC version 7.4.0, version 7.2.3 and below, version 7.1.4 and below, 7.0 all versions, 6.2 all versions may allow an authenticated attacker to obtain sensitive data via crafted HTTP or HTTPs requests.	6.5	More Details
CVE-2025-57563	A path traversal in StarNet Communications Corporation FastX v.4 through v4.1.51 allows unauthenticated attackers to read arbitrary files.	6.5	More Details
CVE-2025-56747	Creativeitem Academy LMS up to and including 5.13 contains a privilege escalation vulnerability in the Api_instructor controller where regular authenticated users can access instructor-only functions without proper role validation, allowing unauthorized course creation and management.	6.5	More Details
CVE-2025-54267	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Incorrect Authorization vulnerability. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized access to elevated privileges that increase integrity impact to high. Exploitation of this issue does not require user interaction.	6.5	More Details
CVE-2025-59185	External control of file name or path in Windows Core Shell allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-60828	WukongCRM-9.0-JAVA was discovered to contain a fastjson deserialization vulnerability via the /OaExamine/setOaExamine interface.	6.5	More Details
CVE-2025-60830	redragon-erp v1.0 was discovered to contain a Shiro deserialization vulnerability caused by the default Shiro key.	6.5	More Details
CVE-2025-60834	A fastjson deserialization vulnerability in uzy-ssm-mall v1.1.0 allows attackers to execute arbitrary code via supplying a crafted input.	6.5	More Details
CVE-2025-42706	A logic error exists in the Falcon sensor for Windows that could allow an attacker, with the prior ability to execute code on a host, to delete arbitrary files. CrowdStrike released a security fix for this issue in Falcon sensor for Windows versions 7.24 and above and all Long Term Visibility (LTV) sensors. There is no indication of exploitation of these issues in the wild. Our threat hunting and intelligence teams are actively monitoring for exploitation and we maintain visibility into any such attempts. The Falcon sensor for Mac, the Falcon sensor for Linux and the Falcon sensor for Legacy Systems are not impacted by this. CrowdStrike was made aware of this issue through our HackerOne bug bounty program. It was discovered by Cong Cheng and responsibly disclosed.	6.5	More Details
CVE-2025-60833	An XML External Entity (XXE) vulnerability in the /mall/wxpay/pay component of uzy-ssm-mall v1.1.0 allows attackers to execute arbitrary code via supplying crafted XML data.	6.5	More Details
CVE-2025-10175	The WP Links Page plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 4.9.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user to cause a denial of service by uploading specially crafted files using	6.5	More Details

33096	uncontrolled recursion.		
CVE-2025-55700	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-58739	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-58729	Improper validation of specified type of input in Windows Local Session Manager (LSM) allows an authorized attacker to deny service over a network.	6.5	More Details
CVE-2025-37148	A vulnerability in the parsing of ethernet frames in AOS-8 Instant and AOS 10 could allow an unauthenticated remote attacker to conduct a denial of service attack. Successful exploitation could allow an attacker to potentially disrupt network services and require manual intervention to restore functionality.	6.5	More Details
CVE-2025-37137	Arbitrary file deletion vulnerabilities have been identified in the command-line interface of an AOS-8 Controller/Mobility Conductor. Successful exploitation of these vulnerabilities could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	6.5	More Details
CVE-2025-37136	Arbitrary file deletion vulnerabilities have been identified in the command-line interface of an AOS-8 Controller/Mobility Conductor. Successful exploitation of these vulnerabilities could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	6.5	More Details
CVE-2025-22258	A heap-based buffer overflow in Fortinet FortiSRA 1.5.0, 1.4.0 through 1.4.2, FortiPAM 1.5.0, 1.4.0 through 1.4.2, 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiProxy 7.6.0 through 7.6.1, 7.4.0 through 7.4.7, FortiOS 7.6.0 through 7.6.2, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10, 7.0.2 through 7.0.16, FortiSwitchManager 7.2.1 through 7.2.5 allows attackers to escalate their privilege via specially crafted http requests.	6.5	More Details
CVE-2025-58717	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-37135	Arbitrary file deletion vulnerabilities have been identified in the command-line interface of an AOS-8 Controller/Mobility Conductor. Successful exploitation of these vulnerabilities could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	6.5	More Details
CVE-2025-60537	Improper input validation in the component /kafka/ui/serdes/CustomSerdeLoader.java of kafka-ui v0.6.0 to v0.7.2 allows attackers to execute arbitrary code via supplying crafted data.	6.5	More Details
CVE-2025-56426	An issue WebKul Bagisto v.2.3.6 allows a remote attacker to execute arbitrary code via the Cart/Checkout API endpoint, specifically, the price calculation logic fails to validate quantity inputs properly.	6.5	More Details
CVE-2025-62386	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-62388	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
	An Uncontrolled Resource Consumption vulnerability in the Connectivity Fault Management (CFM) daemon and the Connectivity Fault Management Manager (cfmman) of Juniper Networks Junos OS Evolved on PTX10001-36MR, PTX10002-36QDD, PTX10004, PTX10008, PTX10016 allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). An attacker on an adjacent device sending specific valid traffic can cause cfmd to spike the CPU		

CVE-2025-52961	to 100% and cfmman's memory to leak, eventually to cause the FPC crash and restart. Continued receipt and processes of these specific valid packets will sustain the Denial of Service (DoS) condition. An indicator of compromise is to watch for an increase in cfmman memory rising over time by issuing the following command and evaluating the RSS number. If the RSS is growing into GBs then consider restarting the device to temporarily clear memory. user@device> show system processes node fpc<num> detail | match cfmman Example: show system processes node fpc0 detail | match cfmman F S UID PID PPID PGID SID C PRI NI ADDR SZ WCHAN RSS PSR STIME TTY TIME CMD 4 S root 15204 1 15204 15204 0 80 0 - 90802 - 113652 4 Sep25 ? 00:15:28 /usr/bin/cfmman -p /var/pfe -o -c /usr/conf/cfmman-cfg-active.xml This issue affects Junos OS Evolved on PTX10001-36MR, PTX10002-36QDD, PTX10004, PTX10008, PTX10016: * from 23.2R1-EVO before 23.2R2-S4-EVO, * from 23.4 before 23.4R2-S4-EVO, * from 24.2 before 24.2R2-EVO, * from 24.4 before 24.4R1-S2-EVO, 24.4R2-EVO. This issue does not affect Junos OS Evolved on PTX10001-36MR, PTX10002-36QDD, PTX10004, PTX10008, PTX10016 before 23.2R1-EVO.	6.5	More Details
CVE-2025-62385	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-62384	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-62383	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-59252	M365 Copilot Spoofing Vulnerability	6.5	More Details
CVE-2025-59272	Copilot Spoofing Vulnerability	6.5	More Details
CVE-2025-59286	Copilot Spoofing Vulnerability	6.5	More Details
CVE-2025-59259	Improper validation of specified type of input in Windows Local Session Manager (LSM) allows an authorized attacker to deny service over a network.	6.5	More Details
CVE-2025-59257	Improper validation of specified type of input in Windows Local Session Manager (LSM) allows an authorized attacker to deny service over a network.	6.5	More Details
CVE-2025-11623	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-10124	The Booking Manager WordPress plugin before 2.1.15 registers a shortcode that deletes bookings and makes that shortcode available to anyone with contributor and above privileges. When a page containing the shortcode is visited, the bookings are deleted.	6.5	More Details
CVE-2025-61925	Astro is a web framework. Prior to version 5.14.2, Astro reflects the value in `X-Forwarded-Host` in output when using `Astro.url` without any validation. It is common for web servers such as nginx to route requests via the `Host` header, and forward on other request headers. As such as malicious request can be sent with both a `Host` header and an `X-Forwarded-Host` header where the values do not match and the `X-Forwarded-Host` header is malicious. Astro will then return the malicious value. This could result in any usages of the `Astro.url` value in code being manipulated by a request. For example if a user follows guidance and uses `Astro.url` for a canonical link the canonical link can be manipulated to another site. It is theoretically possible that the value could also be used as a login/registration or other form	6.5	More Details

	URL as well, resulting in potential redirecting of login credentials to a malicious party. As this is a per-request attack vector the surface area would only be to the malicious user until one considers that having a caching proxy is a common setup, in which case any page which is cached could persist the malicious value for subsequent users. Many other frameworks have an allowlist of domains to validate against, or do not have a case where the headers are reflected to avoid such issues. This could affect anyone using Astro in an on-demand/dynamic rendering mode behind a caching proxy. Version 5.14.2 contains a fix for the issue.		
CVE-2025-59244	External control of file name or path in Windows Core Shell allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-52632	A Missing Secure Attribute in Encrypted Session (SSL) Cookie vulnerability in HCL AION.This issue affects AION: 2.0.	6.5	More Details
CVE-2025-61505	e107 CMS thru 2.3.3 are vulnerable to insecure deserialization in the `install.php` script. The script processes user-controlled input in the `previous_steps` POST parameter using `unserialize(base64_decode())` without validation, allowing attackers to craft malicious serialized data. This could lead to remote code execution, arbitrary file operations, or denial of service, depending on available PHP object gadgets in the codebase.	6.5	More Details
CVE-2025-60268	An arbitrary file upload vulnerability exists in JeeWMS 20250820, which is caused by the lack of file checking in the saveFiles function in /jeewms/cgUploadController.do. An attacker with normal privileges was able to upload a malicious file that would lead to remote code execution.	6.5	More Details
CVE-2025-59214	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-60868	The Alt Redirect 1.6.3 addon for Statamic fails to consistently strip query string parameters when the "Query String Strip" feature is enabled. Case variations, encoded keys, and duplicates are not removed, allowing attackers to bypass sanitization. This may lead to cache poisoning, parameter pollution, or denial of service.	6.5	More Details
CVE-2025-61152	python-jose thru 3.3.0 allows JWT tokens with 'alg=none' to be decoded and accepted without any cryptographic signature verification. A malicious actor can craft a forged token with arbitrary claims (e.g., is_admin=true) and bypass authentication checks, leading to privilege escalation or unauthorized access in applications that rely on python-jose for token validation. This issue is exploitable unless developers explicitly reject 'alg=none' tokens, which is not enforced by the library.	6.5	More Details
CVE-2025-62387	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-60838	An arbitrary file upload vulnerability in MCMS v6.0.1 allows attackers to execute arbitrary code via uploading a crafted file.	6.5	More Details
CVE-2025-62389	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-11550	A vulnerability was found in Tenda W12 3.0.0.6(3948). The impacted element is the function wifiScheduledSet of the file /goform/modules of the component HTTP Request Handler. The manipulation of the argument wifiScheduledSet results in null pointer dereference. The attack may be performed from remote. The exploit has been made public and could be used.	6.5	More Details
CVE-2025-60265	In xckk v9.6, there is a SQL injection vulnerability in which the orderBy parameter in user/list is not securely filtered, resulting in a SQL injection vulnerability.	6.5	More Details
	An arbitrary file download vulnerability in the web interface of Juniper Networks Junos Space		

CVE-2025-59976	allows a network-based authenticated attacker using a crafted GET method to access any file on the file system. Using specially crafted GET methods, an attacker can gain access to files beyond the file path normally allowed by the JBoss daemon. These files could contain sensitive information restricted from access by low-privileged users.This issue affects all versions of Junos Space before 24.1R3.	6.5	More Details
CVE-2025-59967	A NULL Pointer Dereference vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved on ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7348, ACX7509 devices allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). Whenever specific valid multicast traffic is received on any layer 3 interface the evo-pfemand process crashes and restarts. Continued receipt of specific valid multicast traffic results in a sustained Denial of Service (DoS) attack. This issue affects Junos OS Evolved on ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7348, ACX7509: * from 23.2R2-EVO before 23.2R2-S4-EVO, * from 23.4R1-EVO before 23.4R2-EVO. This issue affects IPv4 and IPv6. This issue does not affect Junos OS Evolved ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7348, ACX7509 versions before 23.2R2-EVO.	6.5	More Details
CVE-2025-60266	In xckk v9.6, there is a SQL injection vulnerability in which the orderBy parameter in address/list is not securely filtered, resulting in a SQL injection vulnerability.	6.5	More Details
CVE-2025-59980	An Authentication Bypass by Primary Weakness in the FTP server of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to get limited read-write access to files on the device. When the FTP server is enabled and a user named "ftp" or "anonymous" is configured, that user can login without providing the configured password and then has read-write access to their home directory. This issue affects Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2.	6.5	More Details
CVE-2025-59958	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated, network-based attacker to cause impact to confidentiality and availability. When an output firewall filter is configured with one or more terms where the action is 'reject', packets matching these terms are erroneously sent to the Routing Engine (RE) and further processed there. Processing of these packets will consume limited RE resources. Also responses from the RE back to the source of this traffic could reveal confidential information about the affected device. This issue only applies to firewall filters applied to WAN or revenue interfaces, so not the mgmt or lo0 interface of the routing-engine, nor any input filters. This issue affects Junos OS Evolved on PTX Series: * all versions before 22.4R3-EVO, * 23.2 versions before 23.2R2-EVO.	6.5	More Details
CVE-2025-62392	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-60267	In xckk v9.6, there is a SQL injection vulnerability in which the cond parameter in notice/list is not securely filtered, resulting in a SQL injection vulnerability.	6.5	More Details
CVE-2025-62391	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-62390	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2025-54603	An incorrect OIDC authentication flow in Claroty Secure Access 3.3.0 through 4.0.2 can result in unauthorized user creation or impersonation of existing OIDC users.	6.5	More Details
CVE-2025-9371	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘page_title’ parameter in all versions up to, and including, 28.1.6 due to insufficient input sanitization and output escaping of theme breadcrumbs. 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-2025-7781	The WP JobHunt plugin for WordPress, used by the JobCareer theme, is vulnerable to Stored Cross-Site Scripting via the ‘cs_job_title’ parameter in all versions up to, and including, 7.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Candidate-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-2025-58324	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiSIEM 7.2.0 through 7.2.2, 7.1 all versions, 7.0 all versions, 6.7 all versions, 6.6 all versions, 6.5 all versions, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated attacker to perform a stored cross site scripting (XSS) attack via crafted HTTP requests.	6.4	More Details
CVE-2025-62374	Parse Javascript SDK provides access to the powerful Parse Server backend from your JavaScript app. Prior to 7.0.0, injection of malicious payload allows attacker to remotely execute arbitrary code. ParseObject.fromJSON, ParseObject.pin, ParseObject.registerSubclass, ObjectStateMutations (internal), and encode/decode (internal) are affected. This vulnerability is fixed in 7.0.0.	6.4	More Details
CVE-2025-11197	The Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'drafts' shortcode in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9496	The Enable Media Replace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file_modified shortcode in all versions up to, and including, 4.1.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-35053	Newforma Info Exchange (NIX) accepts requests to '/UserWeb/Common/MarkupServices.ashx' specifying the 'DownloadExportedPDF' command that allow an authenticated user to read and delete arbitrary files with 'NT AUTHORITY\NetworkService' privileges. In Newforma before 2023.1, anonymous access is enabled by default (CVE-2025-35062), allowing an otherwise unauthenticated attacker to effectively authenticate as 'anonymous' and exploit this file upload vulnerability.	6.4	More Details
CVE-2025-9560	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's colibri_newsletter shortcode in all versions up to, and including, 1.0.334 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-2025-10129	The WordPress Live Webcam Widget & Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'webcam' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10167	The Stock History & Reports Manager for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'alg_wc_stock_snapshot_restocked shortcode in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10190	The WP Easy Toggles plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'toggles' shortcode in all versions up to, and including, 1.9.0 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
	HAProxy Kubernetes Ingress Controller before 3.1.13, when the config-snippets feature flag is		

CVE-2025-59303	used, accepts config snippets from users with create/update permissions. This can result in obtaining an ingress token secret as a response. The fixed versions of HAProxy Enterprise Kubernetes Ingress Controller are 3.0.16-ee1, 1.11.13-ee1, and 1.9.15-ee1.	6.4	More Details
CVE-2025-7652	The Easy Plugin Stats plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'eps' shortcode in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-48813	Use of a key past its expiration date in Virtual Secure Mode allows an authorized attacker to perform spoofing locally.	6.3	More Details
CVE-2025-43991	SupportAssist for Home PCs versions 4.8.2 and prior and SupportAssist for Business PCs versions 4.5.3 and prior, contain an UNIX Symbolic Link (Symlink) following vulnerability. A low privileged attacker with local access to the system could potentially exploit this vulnerability to delete arbitrary files only in that affected system.	6.3	More Details
CVE-2025-11667	A vulnerability was found in code-projects Automated Voting System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add_candidate_modal.php.. The manipulation of the argument firstname results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11630	A vulnerability was found in RainyGao DocSys up to 2.02.36. Affected is the function updateRealDoc of the file /Doc/uploadDoc.do of the component File Upload. Performing manipulation of the argument path results in path traversal. The attack can 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.	6.3	More Details
CVE-2025-11629	A vulnerability has been found in RainyGao DocSys up to 2.02.36. This impacts the function getUserList of the file /Manage/getUserList.do. Such manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11646	A vulnerability was detected in Tomofun Furbo 360 and Furbo Mini. This vulnerability affects unknown code of the component GATT Service. The manipulation results in improper access controls. The attack can only be performed from the local network. The exploit is now public and may be used. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11417	A weakness has been identified in Campcodes Advanced Online Voting Management System 1.0. This vulnerability affects unknown code of the file /admin/voters_add.php. Executing manipulation of the argument photo can lead to unrestricted upload. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11553	A weakness has been identified in code-projects Courier Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add-courier.php. Executing manipulation of the argument Shippername can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11486	A vulnerability was identified in SourceCodester Farm Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /buyNow.php. Such manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11436	A vulnerability was detected in JhumanJ OpnForm up to 1.9.3. Affected by this issue is some unknown functionality of the file /answer. The manipulation results in unrestricted upload. The attack can be launched remotely. The exploit is now public and may be used. The patch is identified as 95c3e23856465d202e6aec10bdb6ee0688b5305a. It is advisable to implement a patch to correct this issue.	6.3	More Details
	A vulnerability has been found in JhumanJ OpnForm up to 1.9.3. This vulnerability affects		

CVE-2025-11438	unknown code of the file /custom-domains of the component API Endpoint. Such manipulation leads to missing authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is beb153ce52dceb971c1518f98333328c95f1ba20. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2025-11445	A vulnerability was detected in Kilo Code up to 4.86.0. Affected is the function ClineProvider of the file src/core/webview/ClineProvider.ts of the component Prompt Handler. Performing manipulation results in injection. The attack can be initiated remotely. The exploit is now public and may be used. Applying a patch is the recommended action to fix this issue.	6.3	More Details
CVE-2025-11593	A flaw has been found in CodeAstro Gym Management System 1.0. This vulnerability affects unknown code of the file /admin/actions/delete-equipment.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-11592	A vulnerability was detected in CodeAstro Gym Management System 1.0. This affects an unknown part of the file /admin/edit-equipmentform.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-11591	A security vulnerability has been detected in CodeAstro Gym Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/actions/delete-member.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-11469	A weakness has been identified in SourceCodester Hotel and Lodge Management System 1.0. The affected element is an unknown function of the file /pages/save_customer.php. Executing manipulation of the argument Contact can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11474	A vulnerability was found in SourceCodester Hotel and Lodge Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit_booking.php. Performing manipulation of the argument Name results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11590	A weakness has been identified in CodeAstro Gym Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/equipment-entry.php. Executing manipulation of the argument ename can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11589	A security flaw has been discovered in CodeAstro Gym Management System 1.0. Affected is an unknown function of the file /admin/user-payment.php. Performing manipulation of the argument plan results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-11588	A vulnerability was identified in CodeAstro Gym Management System 1.0. This impacts an unknown function of the file /customer/index.php. Such manipulation of the argument fullname leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11478	A weakness has been identified in SourceCodester Farm Management System 1.0. This issue affects some unknown processing of the file /myCart.php. This manipulation of the argument pid causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11487	A security flaw has been discovered in SourceCodester Farm Management System 1.0. Affected by this issue is some unknown functionality of the file /uploadProduct.php. Performing manipulation of the argument Type results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-11426	A security flaw has been discovered in projectworlds Advanced Library Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit_book.php. The manipulation of the argument image results in unrestricted upload. 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-2025-11490	A vulnerability has been found in wonderwhy-er DesktopCommanderMCP up to 0.2.13. The affected element is the function extractBaseCommand of the file src/command-manager.ts of the component Absolute Path Handler. Such manipulation leads to os command injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor explains: "The usual use case is that AI is asked to do something, picks commands itself, and typically uses simple command names without absolute paths. It's curious why a user would ask the model to bypass restrictions this way. (...) This could potentially be a problem, but we are yet to hear reports of this being an issue in actual workflows. We'll leave this issue open for situations where people may report this as a problem for the long term."	6.3	More Details
CVE-2025-11554	A security vulnerability has been detected in Portabilis i-Educar up to 2.9.10. Affected by this issue is some unknown functionality of the file app/Http/Controllers/AccessLevelController.php of the component User Type Handler. The manipulation leads to insecure inherited permissions. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-11491	A vulnerability was found in wonderwhy-er DesktopCommanderMCP up to 0.2.13. The impacted element is the function CommandManager of the file src/command-manager.ts. Performing manipulation results in os command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11552	A vulnerability was identified in code-projects Online Complaint Site 1.0. This impacts an unknown function of the file /admin/category.php. Such manipulation of the argument Category leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11551	A vulnerability was determined in code-projects Student Result Manager 1.0. This affects an unknown function of the file src/students/Database.java. This manipulation of the argument roll/name/gpa causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-11509	A vulnerability was detected in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/product_add.php. Performing manipulation of the argument prod_name results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-11511	A flaw has been found in code-projects E-Commerce Website 1.0. Affected is an unknown function of the file /pages/supplier_add.php. Executing manipulation of the argument supp_email 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-2025-11514	A vulnerability was identified in code-projects Online Complaint Site 1.0. This vulnerability affects unknown code of the file /cms/users/index.php. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11515	A security flaw has been discovered in code-projects Online Complaint Site 1.0. This issue affects some unknown processing of the file /cms/users/register-complaint.php. Performing manipulation of the argument cid results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-11516	A weakness has been identified in code-projects Online Complaint Site 1.0. Impacted is an unknown function of the file /cms/users/complaint-details.php. Executing manipulation of the argument cid can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11523	A vulnerability was detected in Tenda AC7 15.03.06.44. This vulnerability affects unknown code of the file /goform/AdvSetLanip. The manipulation of the argument lanIp results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-	A weakness has been identified in code-projects Online Complaint Site 1.0. Affected is an unknown function of the file /cms/admin/state.php. This manipulation of the argument state causes sql injection. The attack is possible to be carried out remotely. The exploit has been	6.3	More Details

11530	made available to the public and could be exploited.		
CVE-2025-11431	A vulnerability was determined in code-projects Web-Based Inventory and POS System 1.0. The impacted element is an unknown function of the file /transaction.php. This manipulation of the argument shopid causes sql 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-2025-11481	A flaw has been found in varunsardana004 Blood-Bank-And-Donation-Management-System up to dc9e0393d826fbc85fad9755b5bc12cba1919df2. The impacted element is an unknown function of the file /donate_blood.php. Executing manipulation of the argument fullname can lead to sql injection. The attack may be performed from remote. The exploit has been published and may 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-2025-11597	A vulnerability was identified in code-projects E-Commerce Website 1.0. The impacted element is an unknown function of the file /pages/product_add_qty.php. The manipulation of the argument prod_id leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11612	A vulnerability has been found in code-projects Simple Food Ordering System 1.0. This impacts an unknown function of the file /addproduct.php. The manipulation of the argument Category leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-11603	A vulnerability was found in code-projects Simple Food Ordering System 1.0. This vulnerability affects unknown code of the file /editproduct.php. The manipulation of the argument Category results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11605	A vulnerability was identified in code-projects Client Details System 1.0. Impacted is an unknown function of the file /admin/update-profile.php. Such manipulation of the argument uid leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11606	A security flaw has been discovered in iPynch Social Network Website up to b6933b6d7f82c84819abe458ccf0e59d61119541. The affected element is an unknown function of the component Search. Performing manipulation results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited. This product adopts a rolling release strategy to maintain continuous delivery	6.3	More Details
CVE-2025-11607	A weakness has been identified in harry0703 MoneyPrinterTurbo up to 1.2.6. The impacted element is the function upload_music of the file app/controllers/v1/music.py of the component API Endpoint. Executing manipulation of the argument File can lead to path traversal. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11613	A vulnerability was found in code-projects Simple Food Ordering System 1.0. Affected is an unknown function of the file /addcategory.php. The manipulation of the argument cname results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11600	A security vulnerability has been detected in code-projects Simple Food Ordering System 1.0. Affected is an unknown function of the file editcategory.php. Such manipulation of the argument cname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-11610	A security flaw has been discovered in SourceCodester Simple Inventory System 1.0. This issue affects some unknown processing of the file /brand.php. The manipulation of the argument editBrandName results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-	A weakness has been identified in SourceCodester Simple Inventory System 1.0. Impacted is an unknown function of the file /user.php. This manipulation of the argument uemail causes sql injection. The attack is possible to be carried out remotely. The exploit has been made	6.3	More Details

11611	available to the public and could be exploited.		
CVE-2025-54654	Permission control vulnerability in the Gallery module. Successful exploitation of this vulnerability may affect service confidentiality	6.2	More Details
CVE-2025-55334	Cleartext storage of sensitive information in Windows Kernel allows an unauthorized attacker to bypass a security feature locally.	6.2	More Details
CVE-2025-21059	Improper authorization in Samsung Health prior to version 6.30.5.105 allows local attackers to access data in Samsung Health.	6.2	More Details
CVE-2025-62364	text-generation-webui is an open-source web interface for running Large Language Models. In versions through 3.13, a Local File Inclusion vulnerability exists in the character picture upload feature. An attacker can upload a text file containing a symbolic link to an arbitrary file path. When the application processes the upload, it follows the symbolic link and serves the contents of the targeted file through the web interface. This allows an unauthenticated attacker to read sensitive files on the server, potentially exposing system configurations, credentials, and other confidential information. This vulnerability is fixed in 3.14. No known workarounds exist.	6.2	More Details
CVE-2025-58278	Identity authentication bypass vulnerability in the Gallery app. Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2025-37138	An authenticated command injection vulnerability exists in the command line interface binary of AOS-10 GW and AOS-8 Controllers/Mobility Conductor operating system. Exploitation of this vulnerability requires physical access to the hardware controllers. A successful attack could allow an authenticated malicious actor with physical access to execute arbitrary commands as a privileged user on the underlying operating system.	6.2	More Details
CVE-2025-11371	In the default installation and configuration of Gladinet CentreStack and TrioFox, there is an unauthenticated Local File Inclusion Flaw that allows unintended disclosure of system files. Exploitation of this vulnerability has been observed in the wild. This issue impacts Gladinet CentreStack and Triofox: All versions prior to and including 16.7.10368.56560	6.2	More Details
CVE-2025-59258	Insertion of sensitive information into log file in Active Directory Federation Services allows an unauthorized attacker to disclose information locally.	6.2	More Details
CVE-2025-58300	Buffer overflow vulnerability in the device management module. Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2025-58301	Buffer overflow vulnerability in the device management module. Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2025-61319	ReNgine thru 2.2.0 is vulnerable to a Stored Cross-Site Scripting (XSS) vulnerability in the Vulnerabilities module. When scanning a target with an XSS payload, the unsanitized payload is rendered in the ReNgine web UI, resulting in arbitrary JavaScript execution in the victim's browser. This can be abused to steal session cookies, perform unauthorized actions, or compromise the ReNgine administrator's account.	6.1	More Details
CVE-2025-59995	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Quick Template page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-60318	SourceCodester Pet Grooming Management Software 1.0 is vulnerable to Cross Site Scripting (XSS) in /admin/profile.php via the fname (First Name) and lname (Last Name) fields.	6.1	More Details

CVE-2025-59996	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Configuration View page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59997	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the CLI Configlets pages that, when visited by another user, enable the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-55682	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2025-59998	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Archive Log screen that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-11498	An Improper Neutralization of Formula Elements in a CSV File vulnerability exists in System Diagnostics Manager (SDM) of B&R Automation Runtime versions before 6.4 enabling a remote attacker to inject formula data into a generated CSV file. The exploitation of this vulnerability requires the attacker to create a malicious link. The user would need to click on this link, after which the resulting CSV file addi-tionally needs to be manually opened.	6.1	More Details
CVE-2025-59999	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the API Access Profiles page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-60302	code-projects Client Details System 1.0 is vulnerable to Cross Site Scripting (XSS). When adding customer information, the client details system fills in malicious JavaScript code in the username field.	6.1	More Details
CVE-2024-44088	Malicious script injection ('Cross-site Scripting') vulnerability in Apache Geode web-api (REST). This vulnerability allows an attacker that tricks a logged-in user into clicking a specially-crafted link to execute code on the returned page, which could lead to theft of the user's session information and even account takeover. This issue affects Apache Geode: all versions prior to 1.15.2 Users are recommended to upgrade to version 1.15.2, which fixes the issue.	6.1	More Details
CVE-2025-61532	Cross Site Scripting vulnerability in SVX Portal v.2.7A to execute arbitrary code via the TG parameter on last_heard_page.php component	6.1	More Details
CVE-2025-60001	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Generate Report page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-55338	Missing Ability to Patch ROM Code in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2025-55337	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2025-	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Template Definitions page that, when visited by another user, enables the attacker to execute	6.1	More

60002	commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.		Details
CVE-2025-60009	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the CLI Configlet page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-10357	The Simple SEO WordPress plugin before 2.0.32 does not sanitise and escape some parameters when outputing them in the page, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks.	6.1	More Details
CVE-2025-55333	Incomplete comparison with missing factors in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2025-55332	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2025-55330	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2025-60304	code-projects Simple Scheduling System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Subject Description field.	6.1	More Details
CVE-2025-27045	Information disclosure while processing batch command execution in Video driver.	6.1	More Details
CVE-2025-60000	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Generate Report page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59994	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Quick Template page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-8887	Authorization Bypass Through User-Controlled Key, Missing Authorization, Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Usta Information Systems Inc. Aybs Interaktif allows Forceful Browsing, Parameter Injection, Input Data Manipulation.This issue affects Aybs Interaktif: from 2024 through 28082025.	6.1	More Details
CVE-2025-61183	Cross Site Scripting in vaahcms v.2.3.1 allows a remote attacker to execute arbitrary code via upload method in the storeAvatar() method of UserBase.php	6.1	More Details
CVE-2025-59981	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Device Template Definition page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59982	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the dashboard search field that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details

CVE-2025-59993	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Space Node Setting fields that, when visited by another user, enable the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-52647	The BigFix WebUI application responds with HOST information from the HTTP header field making it vulnerable to Host Header Poisoning Attacks.	6.1	More Details
CVE-2025-59984	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in Global Search that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59985	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in a field on the Purging Policy page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59986	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the input fields in Model Devices that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59987	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the arbitrary device search field that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59983	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Template Definition page, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59988	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Generate Report page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59989	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Device Discovery page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59990	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the template creation pages that, when visited by another user, enable the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-59991	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Device Management pages that, when visited by another user, enable the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')		

CVE-2025-59992	vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the Secure Console page that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R4.	6.1	More Details
CVE-2025-60313	Sourcecodester Link Status Checker 1.0 is vulnerable to a Cross-Site Scripting (XSS) in the Enter URLs to check input field. This allows a remote attacker to execute arbitrary code.	6.1	More Details
CVE-2025-0033	Improper access control within AMD SEV-SNP could allow an admin privileged attacker to write to the RMP during SNP initialization, potentially resulting in a loss of SEV-SNP guest memory integrity.	6.0	More Details
CVE-2025-37139	A vulnerability in an AOS firmware binary allows an authenticated malicious actor to permanently delete necessary boot information. Successful exploitation may render the system unbootable, resulting in a Denial of Service that can only be resolved by replacing the affected hardware.	6.0	More Details
CVE-2025-37149	A potential out-of-bound reads vulnerability in HPE ProLiant RL300 Gen11 Server's UEFI firmware.	6.0	More Details
CVE-2025-58295	Buffer overflow vulnerability in the development framework module. Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2025-35058	Newforma Info Exchange (NIX) '/UserWeb/Common/MarkupServices.ashx' allows a remote, unauthenticated attacker to cause NIX to make an SMB connection to an attacker-controlled system. The attacker can capture the NTLMv2 hash of the customer-configured NIX service account.	5.9	More Details
CVE-2025-54265	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Incorrect Authorization vulnerability. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction.	5.9	More Details
CVE-2025-35061	Newforma Info Exchange (NIX) '/NPCSRemoteWeb/LegacyIntegrationServices.asmx' allows a remote, unauthenticated attacker to cause NIX to make an SMB connection to an attacker-controlled system. The attacker can capture the NTLMv2 hash of the user-configured NIX service account.	5.9	More Details
CVE-2025-11380	The Everest Backup – WordPress Cloud Backup, Migration, Restore & Cloning Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'everest_process_status' AJAX action in all versions up to, and including, 2.3.5. This makes it possible for unauthenticated attackers to retrieve back-up file locations that can be subsequently accessed and downloaded. This does require a back-up to be running in order for an attacker to retrieve the back-up location.	5.9	More Details
CVE-2025-58284	Permission control vulnerability in the network module. Successful exploitation of this vulnerability may affect service confidentiality.	5.9	More Details
CVE-2025-58297	Buffer overflow vulnerability in the sensor service. Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2025-52960	A Buffer Copy without Checking Size of Input vulnerability in the Session Initialization Protocol (SIP) ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When memory utilization is high, and specific SIP packets are received, flowd crashes. While the system recovers automatically, the disruption can significantly impact service stability. Continuous receipt of these specific SIP packets, while high utilization is present, will cause a sustained DoS condition. The utilization is outside the attackers control, so they would not be able to deterministically exploit this. This issue affects Junos OS on SRX Series and MX Series: * All versions before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S5, *	5.9	More Details

	from 24.2 before 24.2R2.		
CVE-2025-58289	Vulnerability of improper exception handling in the print module. Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2025-61780	Rack is a modular Ruby web server interface. Prior to versions 2.2.20, 3.1.18, and 3.2.3, a possible information disclosure vulnerability existed in `Rack::Sendfile` when running behind a proxy that supports `x-sendfile` headers (such as Nginx). Specially crafted headers could cause `Rack::Sendfile` to miscommunicate with the proxy and trigger unintended internal requests, potentially bypassing proxy-level access restrictions. When `Rack::Sendfile` received untrusted `x-sendfile-type` or `x-accel-mapping` headers from a client, it would interpret them as proxy configuration directives. This could cause the middleware to send a "redirect" response to the proxy, prompting it to reissue a new internal request that was not subject to the proxy's access controls. An attacker could exploit this by setting a crafted `x-sendfile-type: x-accel-redirect` header, setting a crafted `x-accel-mapping` header, and requesting a path that qualifies for proxy-based acceleration. Attackers could bypass proxy-enforced restrictions and access internal endpoints intended to be protected (such as administrative pages). The vulnerability did not allow arbitrary file reads but could expose sensitive application routes. This issue only affected systems meeting all of the following conditions: The application used `Rack::Sendfile` with a proxy that supports `x-accel-redirect` (e.g., Nginx); the proxy did **not** always set or remove the `x-sendfile-type` and `x-accel-mapping` headers; and the application exposed an endpoint that returned a body responding to `.to_path`. Users should upgrade to Rack versions 2.2.20, 3.1.18, or 3.2.3, which require explicit configuration to enable `x-accel-redirect`. Alternatively, configure the proxy to always set or strip the header, or in Rails applications, disable sendfile completely.	5.8	More Details
CVE-2025-31365	An Improper Control of Generation of Code ('Code Injection') vulnerability [CWE-94] in FortiClientMac 7.4.0 through 7.4.3, 7.2.1 through 7.2.8 may allow an unauthenticated attacker to execute arbitrary code on the victim's host via tricking the user into visiting a malicious website.	5.8	More Details
CVE-2025-2140	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user on the network to spoof email identity of the sender due to improper verification of source data.	5.7	More Details
CVE-2025-21044	Out-of-bounds write in fingerprint trustlet prior to SMR Oct-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.	5.7	More Details
CVE-2025-37727	Insertion of sensitive information in log file in Elasticsearch can lead to loss of confidentiality under specific preconditions when auditing requests to the reindex API https://www.elastic.co/docs/api/doc/elasticsearch/operation/operation-reindex	5.7	More Details
CVE-2025-11648	A vulnerability has been found in Tomofun Furbo 360 and Furbo Mini. Impacted is an unknown function of the file TF_FQDN.json of the component GATT Interface URL Handler. Such manipulation leads to server-side request forgery. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2025-11636	A security vulnerability has been detected in Tomofun Furbo 360 up to FB0035_FW_036. This issue affects some unknown processing of the component Account Handler. Such manipulation leads to server-side request forgery. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2025-42701	A race condition exists in the Falcon sensor for Windows that could allow an attacker, with the prior ability to execute code on a host, to delete arbitrary files. CrowdStrike released a security fix for this issue in Falcon sensor for Windows versions 7.24 and above and all Long Term Visibility (LTV) sensors. There is no indication of exploitation of these issues in the wild. Our threat hunting and intelligence team are actively monitoring for exploitation and we maintain visibility into any such attempts. The Falcon sensor for Mac, the Falcon sensor for	5.6	More Details

	Linux and the Falcon sensor for Legacy Systems are not impacted by this. CrowdStrike was made aware of this issue through our HackerOne bug bounty program. It was discovered by Cong Cheng and responsibly disclosed.		
CVE-2025-27041	Transient DOS while processing video packets received from video firmware.	5.5	More Details
CVE-2025-20724	In wlan AP driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00418894; Issue ID: MSV-3475.	5.5	More Details
CVE-2025-47979	Insertion of sensitive information into log file in Windows Failover Cluster allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-20722	In gnss driver, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09920036; Issue ID: MSV-3798.	5.5	More Details
CVE-2025-59186	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-54275	Substance3D - Viewer versions 0.25.2 and earlier are affected by an out-of-bounds write vulnerability that could lead to application denial-of-service. An attacker could leverage this vulnerability to crash the application or make it unavailable. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-21060	Cleartext storage of sensitive information in Smart Switch prior to version 3.7.67.2 allows local attackers to access backup data from applications. User interaction is required for triggering this vulnerability.	5.5	More Details
CVE-2025-59188	Exposure of sensitive information to an unauthorized actor in Windows Failover Cluster allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-55699	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-59184	Exposure of sensitive information to an unauthorized actor in Windows High Availability Services allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-58293	Vulnerability of improper exception handling in the print module. Successful exploitation of this vulnerability may affect availability.	5.5	More Details
CVE-2025-58283	Permission control vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2025-59190	Improper input validation in Microsoft Windows Search Component allows an unauthorized attacker to deny service locally.	5.5	More Details
CVE-2025-55695	Out-of-bounds read in Windows WLAN Auto Config Service allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-59197	Insertion of sensitive information into log file in Windows ETL Channel allows an authorized attacker to disclose information locally.	5.5	More Details

CVE-2025-11626	MONGO dissector infinite loop in Wireshark 4.4.0 to 4.4.9 and 4.2.0 to 4.2.13 allows denial of service	5.5	More Details
CVE-2025-59203	Insertion of sensitive information into log file in Windows StateRepository API allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-59204	Use of uninitialized resource in Windows Management Services allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-59211	Exposure of sensitive information to an unauthorized actor in Windows Push Notification Core allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-55683	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-59229	Uncaught exception in Microsoft Office allows an unauthorized attacker to deny service locally.	5.5	More Details
CVE-2025-59209	Exposure of sensitive information to an unauthorized actor in Windows Push Notification Core allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-55676	Generation of error message containing sensitive information in Windows USB Video Driver allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-55336	Exposure of sensitive information to an unauthorized actor in Windows Cloud Files Mini Filter Driver allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-35060	Newforma Info Exchange (NIX) provides a 'Send a File Transfer' feature that allows a remote, authenticated attacker to upload SVG files that contain JavaScript or other content that may be executed or rendered by a web browser using a mobile user agent.	5.5	More Details
CVE-2025-55325	Buffer over-read in Windows Storage Management Provider allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-43296	A logic issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26. An app may bypass Gatekeeper checks.	5.5	More Details
CVE-2025-59260	Exposure of sensitive information to an unauthorized actor in Microsoft Failover Cluster Virtual Driver allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-59253	Improper access control in Microsoft Windows Search Component allows an authorized attacker to deny service locally.	5.5	More Details
CVE-2025-58288	Denial of service (DoS) vulnerability in the office service. Successful exploitation of this vulnerability may affect availability.	5.5	More Details
CVE-2025-27049	Transient DOS while processing IOCTL call for image encoding.	5.5	More Details
CVE-2025-	Improper access control in SecSettings prior to SMR Oct-2025 Release 1 allows local attackers	5.5	More

21049	to access sensitive information. User interaction is required for triggering this vulnerability.		Details
CVE-2025-33177	NVIDIA Jetson Linux and IGX OS contain a vulnerability in NvMap, where improper tracking of memory allocations could allow a local attacker to cause memory overallocation. A successful exploitation of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2025-62358	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.1, the log parameter in configuracao_geral.php is vulnerable to Reflected Cross-Site Scripting (XSS). An attacker can inject arbitrary JavaScript, which executes in the victim's browser. This vulnerability is fixed in 3.5.1.	5.4	More Details
CVE-2025-61797	Adobe Experience Manager versions 11.6 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	5.4	More Details
CVE-2025-42901	SAP Application Server for ABAP allows an authenticated attacker to store malicious JavaScript payloads which could be executed in victim user's browser when accessing the affected functionality of BAPI explorer. This has low impact on confidentiality and integrity with no impact on availability of the application.	5.4	More Details
CVE-2025-11166	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in all versions up to, and including, 9.0.46. This is due to the plugin exposing state-changing REST actions through an AJAX bridge without proper CSRF token validation, and having destructive logic reachable via GET requests with no permission_callback. This makes it possible for unauthenticated attackers to force logged-in administrators to create, update, or delete markers and geometry features via CSRF attacks, and allows anonymous users to trigger mass deletion of markers via unsafe GET requests.	5.4	More Details
CVE-2025-11190	The Kiwire Captive Portal contains an open redirection issue via the login-url parameter, allowing an attacker to redirect users to an attacker controlled website.	5.4	More Details
CVE-2025-52624	A vulnerability Bypass of the script allowlist configuration in HCL AION. An incorrectly configured Content-Security-Policy header may allow unauthorized scripts to execute, increasing the risk of cross-site scripting and other injection-based attacks.This issue affects AION: 2.0.	5.4	More Details
CVE-2025-42908	Due to a Cross-Site Request Forgery (CSRF) vulnerability in SAP NetWeaver Application Server for ABAP, an authenticated attacker could initiate transactions directly via the session manager, bypassing the first transaction screen and the associated authorization check. This vulnerability could allow the attacker to perform actions and execute transactions that would normally require specific permissions, compromising the integrity and confidentiality of the system by enabling unauthorized access to restricted functionality. There is no impact to availability from this vulnerability.	5.4	More Details
CVE-2025-60298	Novel-Plus up to 5.2.4 was discovered to contain a Stored Cross-Site Scripting (XSS) vulnerability via the /author/updateIndexName endpoint. This vulnerability allows authenticated attackers to inject malicious JavaScript code through the indexName parameter, which gets stored in the database and executed when other users view the affected book chapter.	5.4	More Details
CVE-2025-11616	A missing validation check in FreeRTOS-Plus-TCP's ICMPv6 packet processing code can lead to an out-of-bounds read when receiving ICMPv6 packets of certain message types which are smaller than the expected size. These issues only affect applications using IPv6. Users should upgrade to the latest version and ensure any forked or derivative code is patched to incorporate the new fixes.	5.4	More Details
CVE-	Opencast is a free, open-source platform to support the management of educational audio and video content. Prior to Opencast 17.8 and 18.2, the paella would include and render some user inputs (metadata like title, description, etc.) unfiltered and unmodified. The vulnerability allows attackers to inject and malicious HTML and JavaScript in the player, which would then		

2025-61788	be executed in the browsers of users watching the prepared media. This can then be used to modify the site or to execute actions in the name of logged-in users. To inject malicious metadata, an attacker needs write access to the system. For example, the ability to upload media and modify metadata. This cannot be exploited by unauthenticated users. This issue is fixed in Opencast 17.8 and 18.2.	5.4	More Details
CVE-2025-60010	A password aging vulnerability in the RADIUS client of Juniper Networks Junos OS and Junos OS Evolved allows an authenticated, network-based attacker to access the device without enforcing the required password change. Affected devices allow logins by users for whom the RADIUS server has responded with a reject and required the user to change the password as their password was expired. Therefore the policy mandating the password change is not enforced. This does not allow users to login with a wrong password, but only with the correct but expired one. This issue affects: Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2-S1, * 24.4 versions before 24.4R1-S3, 24.4R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * 23.2 versions before 23.2R2-S4-EVO, * 23.4 versions before 23.4R2-S5-EVO, * 24.2 versions before 24.2R2-S1-EVO, * 24.4 versions before 24.4R1-S3-EVO, 24.4R2-EVO.	5.4	More Details
CVE-2025-59428	EspoCRM is an open source customer relationship management application. In versions before 9.1.9, a vulnerability allows arbitrary user creation, including administrative accounts, through a combination of stored SVG injection and lack of CSRF protection. An attacker with Knowledge Base edit permissions can embed a malicious SVG element containing a link in the body field of an article. When an authenticated user clicks the malicious link, they are redirected to an attacker-controlled HTML page that executes a CSRF request against the api/v1/User endpoint. If the victim is prompted for and enters their credentials, an attacker-controlled account is created with privileges determined by the CSRF payload. This issue has been patched in version 9.1.9.	5.4	More Details
CVE-2025-11631	A vulnerability was determined in RainyGao DocSys up to 2.02.36. Affected by this vulnerability is an unknown functionality of the file /Doc/deleteDoc.do. Executing manipulation of the argument path can lead to path traversal. The attack can 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.	5.4	More Details
CVE-2025-54272	Adobe Experience Manager versions 11.6 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	5.4	More Details
CVE-2025-60314	Configuroweb Sistema Web de Inventario 1.0 is vulnerable to a Stored Cross-Site Scripting (XSS) due to the lack of input sanitization on the product name parameter (Nombre:Producto) allowing an authenticated attacker to inject malicious payloads and execute arbitrary JavaScript.	5.4	More Details
CVE-2025-7374	The WP JobHunt plugin for WordPress, used by the JobCareer theme, is vulnerable to authorization bypass in all versions up to, and including, 7.6. This is due to insufficient login restrictions on inactive and pending accounts. This makes it possible for authenticated attackers, with Candidate- and Employer-level access and above, to log in to the site even if their account is inactive or pending.	5.4	More Details
CVE-2025-61796	Adobe Experience Manager versions 11.6 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	5.4	More Details
CVE-2025-11617	A missing validation check in FreeRTOS-Plus-TCP's IPv6 packet processing code can lead to an out-of-bounds read when receiving a IPv6 packet with incorrect payload lengths in the packet header. This issue only affects applications using IPv6. We recommend users upgrade to the latest version and ensure any forked or derivative code is patched to incorporate the new	5.4	More Details

	fixes.		
CVE-2025-60299	Novel-Plus with 5.2.0 was discovered to contain a Stored Cross-Site Scripting (XSS) vulnerability via the /book/addCommentReply endpoint. An authenticated user can inject malicious JavaScript through the replyContent parameter when replying to a book comment. The payload is stored in the database and is executed in other users' browsers when they view the affected comment thread.	5.4	More Details
CVE-2025-54277	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Incorrect Authorization vulnerability. An attacker could leverage this vulnerability to bypass security measures and gain limited unauthorized read access. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2024-26008	An improper check or handling of exceptional conditions vulnerability [CWE-703] in FortiOS version 7.4.0 through 7.4.3 and before 7.2.7, FortiProxy version 7.4.0 through 7.4.3 and before 7.2.9, FortiPAM before 1.2.0 and FortiSwitchManager version 7.2.0 through 7.2.3 and version 7.0.0 through 7.0.3 fgfm daemon may allow an unauthenticated attacker to repeatedly reset the fgfm connection via crafted SSL encrypted TCP requests.	5.3	More Details
CVE-2025-27906	IBM Content Navigator 3.0.11, 3.0.15, 3.1.0, and 3.2.0 could expose the directory listing of the application upon using an application URL. Application files and folders are visible in the browser to a user; however, the contents of the files cannot be read obtained or modified.	5.3	More Details
CVE-2025-11171	The Chartify – WordPress Chart Plugin for WordPress is vulnerable to Missing Authentication for Critical Function in all versions up to, and including, 3.5.9. This is due to the plugin registering an unauthenticated AJAX action that dispatches to admin-class methods based on a request parameter, without any nonce or capability checks. This makes it possible for unauthenticated attackers to execute administrative functions via the wp-admin/admin-ajax.php endpoint granted they can identify callable method names.	5.3	More Details
CVE-2025-54973	A concurrent execution using shared resource with improper synchronization ('Race Condition') vulnerability [CWE-362] in Fortinet FortiAnalyzer version 7.6.0 through 7.6.2, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10 and before 7.0.13 allows an attacker to attempt to win a race condition to bypass the FortiCloud SSO authorization via crafted FortiCloud SSO requests.	5.3	More Details
CVE-2023-37401	IBM Aspera Faspex 5.0.0 through 5.0.13.1 uses a cross-domain policy file that includes domains that should not be trusted.	5.3	More Details
CVE-2025-42902	Due to the memory corruption vulnerability in SAP NetWeaver AS ABAP and ABAP Platform, an unauthenticated attacker can send a corrupted SAP Logon Ticket or SAP Assertion Ticket to the SAP application server. This leads to a dereference of NULL which makes the work process crash. As a result, it has a low impact on the availability but no impact on the confidentiality and integrity.	5.3	More Details
CVE-2025-35052	Newforma Info Exchange (NIX) uses a hard-coded key to encrypt certain query parameters. Some encrypted parameter values can specify paths to download files, potentially bypassing authentication and authorization, for example, the 'qs' parameter used in '/DownloadWeb/download.aspx'. This key is shared across NIX installations. NIX 2023.3 and 2024.1 limit the use of hard-coded keys.	5.3	More Details
CVE-2025-35054	Newforma Info Exchange (NIX) stores credentials used to configure NPCS in 'HKLM\Software\WOW6432Node\Newforma\<version>\Credentials'. The credentials are encrypted but the encryption key is stored in the same registry location. Authenticated users can access both the credentials and the encryption key. If these are Active Directory credentials, an attacker may be able to gain access to additional systems and resources.	5.3	More Details
CVE-2025-35057	Newforma Info Exchange (NIX) '/RemoteWeb/IntegrationServices.ashx' allows a remote, unauthenticated attacker to cause NIX to make an SMB connection to an attacker-controlled system. The attacker can capture the NTLMv2 hash of the NIX service account.	5.3	More Details
CVE-2025-35062	Newforma Info Exchange (NIX) before version 2023.1 by default allows anonymous authentication which allows an unauthenticated attacker to exploit additional vulnerabilities that require authentication.	5.3	More Details

CVE-2025-59836	Omni manages Kubernetes on bare metal, virtual machines, or in a cloud. Prior to 1.1.5 and 1.0.2, there is a nil pointer dereference vulnerability in the Omni Resource Service allows unauthenticated users to cause a server panic and denial of service by sending empty create/update resource requests through the API endpoints. The vulnerability exists in the isSensitiveSpec function which calls grpcomni.CreateResource without checking if the resource's metadata field is nil. When a resource is created with an empty Metadata field, the CreateResource function attempts to access resource.Metadata.Version causing a segmentation fault. This vulnerability is fixed in 1.1.5 and 1.0.2.	5.3	More Details
CVE-2025-11580	A weakness has been identified in PowerJob up to 5.1.2. This affects the function list of the file /user/list. This manipulation causes missing authorization. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	5.3	More Details
CVE-2025-11581	A security vulnerability has been detected in PowerJob up to 5.1.2. This vulnerability affects unknown code of the file /openApi/runJob of the component OpenAPIController. Such manipulation leads to missing authorization. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2025-11672	Uniweb/SoliPACS WebServer developed by EBM Technologies has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to access a specific page to obtain user group names.	5.3	More Details
CVE-2025-11671	Uniweb/SoliPACS WebServer developed by EBM Technologies has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to access a specific page to obtain information such as account names and IP addresses.	5.3	More Details
CVE-2025-58285	Permission control vulnerability in the media module. Successful exploitation of this vulnerability may affect service confidentiality.	5.3	More Details
CVE-2025-31996	HCL Unica Platform is affected by unprotected files due to improper access controls. These files may contain sensitive information such as private or system information that can be exploited by attackers to compromise the application, infrastructure, or users.	5.3	More Details
CVE-2025-9196	The Trinity Audio – Text to Speech AI audio player to convert content into audio plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.21.0 via the ~/admin/inc/phpinfo.php file that gets created on install. This makes it possible for unauthenticated attackers to extract sensitive data including configuration data.	5.3	More Details
CVE-2025-11518	The WPC Smart Wishlist for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.0.3 via several wishlist AJAX functions due to missing validation on a user controlled key that is exposed when wishlists are shared. This makes it possible for unauthenticated attackers to empty and add to other user's wishlists, if they have access to the key.	5.3	More Details
CVE-2025-11594	A vulnerability has been found in ywxbear PHP-Bookstore-Website-Example and PHP Basic BookStore Website up to 0e0b9f542f7a2d90a8d7f8c83caca69294e234e4. This issue affects some unknown processing of the file /index.php of the component Quantity Handler. Such manipulation leads to improper validation of specified quantity in input. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	5.3	More Details
CVE-2025-8484	The Code Quality Control Tool plugin for WordPress is vulnerable to Sensitive Information Exposure in version 0.1 through publicly exposed log files. This makes it possible for unauthenticated attackers to view potentially sensitive information contained in the exposed log files.	5.3	More Details
CVE-2025-52616	HCL Unica 12.1.10 can expose sensitive system information. An attacker could use this information to form an attack plan by leveraging known vulnerabilities in the application.	5.3	More Details
CVE-2025-11579	github.com/nwaples/rardecode versions <=2.1.1 fail to restrict the dictionary size when reading large RAR dictionary sizes, which allows an attacker to provide a specially crafted RAR file and cause Denial of Service via an Out Of Memory Crash.	5.3	More Details

CVE-2025-42906	SAP Commerce Cloud contains a path traversal vulnerability that may allow users to access web applications such as the Administration Console from addresses where the Administration Console is not explicitly deployed. This could potentially bypass configured access restrictions, resulting in a low impact on confidentiality, with no impact on the integrity or availability of the application.	5.3	More Details
CVE-2025-60006	Multiple instances of an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the CLI of Juniper Networks Junos OS Evolved could be used to elevate privileges and/or execute unauthorized commands. When an attacker executes crafted CLI commands, the options are processed via a script in some cases. These scripts are not hardened so injected commands might be executed via the shell, which allows an attacker to perform operations, which they should not be able to do according to their assigned permissions. This issue affects Junos OS Evolved: * 24.2 versions before 24.2R2-S2-EVO, * 24.4 versions before 24.4R2-EVO. This issue does not affect Junos OS Evolved versions earlier than 24.2R1-EVO.	5.3	More Details
CVE-2025-59962	An Access of Uninitialized Pointer vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved with BGP sharding configured allows an attacker triggering indirect next-hop updates, along with timing outside the attacker's control, to cause rpd to crash and restart, leading to a Denial of Service (DoS). With BGP sharding enabled, triggering route resolution of an indirect next-hop (e.g., an IGP route change over which a BGP route gets resolved), may cause rpd to crash and restart. An attacker causing continuous IGP route churn, resulting in repeated route re-resolution, will increase the likelihood of triggering this issue, leading to a potentially extended DoS condition. This issue affects: Junos OS: * all versions before 21.4R3-S6, * from 22.1 before 22.1R3-S6, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2; Junos OS Evolved: * all versions before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-EVO, * from 23.2 before 23.2R2-EVO. Versions before Junos OS 21.3R1 and Junos OS Evolved 21.3R1-EVO are unaffected by this issue.	5.3	More Details
CVE-2025-41707	The websocket handler is vulnerable to a denial of service condition. An unauthenticated remote attacker can send a crafted websocket message to trigger the issue without affecting the core functionality.	5.3	More Details
CVE-2025-41706	The webserver is vulnerable to a denial of service condition. An unauthenticated remote attacker can craft a special GET request with an over-long content-length to trigger the issue without affecting the core functionality.	5.3	More Details
CVE-2025-41704	An unauthanticated remote attacker can perform a DoS of the Modbus service by sending a specific function and sub-function code without affecting the core functionality.	5.3	More Details
CVE-2025-59288	Improper verification of cryptographic signature in GitHub allows an unauthorized attacker to perform spoofing over an adjacent network.	5.3	More Details
CVE-2025-21047	Improper access control in KnoxGuard prior to SMR Oct-2025 Release 1 allows physical attackers to use the privileged APIs.	5.2	More Details
CVE-2025-55679	Improper input validation in Windows Kernel allows an unauthorized attacker to disclose information locally.	5.1	More Details
CVE-2025-35056	Newforma Info Exchange (NIX) '/UserWeb/Common/MarkupServices.ashx' 'StreamStampImage' accepts an encrypted file path and returns an image of the specified file. An authenticated attacker can read arbitrary files subject to the privileges of NIX, typically 'NT AUTHORITY\NetworkService', and the ability of StreamStampImage to process the file. The encrypted file path can be generated using the shared, hard-coded secret key described in CVE-2025-35052. This vulnerability cannot be exploited as an 'anonymous' user as described in CVE-2025-35062.	5.0	More Details
CVE-2025-59198	Improper input validation in Microsoft Windows Search Component allows an authorized attacker to deny service locally.	5.0	More Details

CVE-2025-37142	Arbitrary file download vulnerabilities exist in the CLI binary of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	4.9	More Details
CVE-2025-10048	The My auctions allegro plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter in all versions up to, and including, 3.6.31 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-37140	Arbitrary file download vulnerabilities exist in the CLI binary of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	4.9	More Details
CVE-2025-37141	Arbitrary file download vulnerabilities exist in the CLI binary of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	4.9	More Details
CVE-2025-37143	An arbitrary file download vulnerability exists in the web-based management interface of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an Authenticated malicious actor to download arbitrary files through carefully constructed exploits.	4.9	More Details
CVE-2025-9950	The Error Log Viewer by BestWebSoft plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.1.6 via the rrrlgvwr_get_file function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2025-37145	Arbitrary file download vulnerabilities exist in a low-level interface library in AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	4.9	More Details
CVE-2025-36171	IBM Aspera Faspex 5.0.0 through 5.0.13.1 could allow a privileged user to cause a denial of service from improperly validated API input due to excessive resource consumption.	4.9	More Details
CVE-2025-37144	Arbitrary file download vulnerabilities exist in a low-level interface library in AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	4.9	More Details
CVE-2025-9947	The Custom 404 Pro plugin for WordPress is vulnerable to time-based SQL Injection via the ‘path’ parameter in all versions up to, and including, 3.12.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-10185	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in the action nf_load_form_entries in all versions up to, and including, 9.1.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This may be exploitable by lower-level users if access is granted by a site administrator.	4.9	More Details
CVE-	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields.		More

2025-54266	Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field. Scope is changed.	4.8	Details
CVE-2025-25252	An Insufficient Session Expiration vulnerability [CWE-613] in FortiOS SSL VPN 7.6.0 through 7.6.2, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10, 7.0.0 through 7.0.16, 6.4 all versions may allow a remote attacker (e.g. a former admin whose account was removed and whose session was terminated) in possession of the SAML record of a user session to access or re-open that session via re-use of SAML record.	4.8	More Details
CVE-2025-55248	Inadequate encryption strength in .NET, .NET Framework, Visual Studio allows an authorized attacker to disclose information over a network.	4.8	More Details
CVE-2025-11655	A security flaw has been discovered in Total.js Flow up to 673ef9144dd25d4f4fd4fdfda5af27f230198924. The impacted element is an unknown function of the component SVG File Handler. Performing manipulation results in unrestricted upload. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-31366	An Improper Neutralization of Input During Web Page Generation vulnerability [CWE-79] in FortiOS 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiProxy 7.6.0 through 7.6.3, 7.4.0 through 7.4.9, 7.2 all versions, 7.0 all versions; FortiSASE 25.3.a may allow an unauthenticated attacker to perform a reflected cross site scripting (XSS) via crafted HTTP requests.	4.7	More Details
CVE-2025-58719	Use after free in Connected Devices Platform Service (Cdpsvc) allows an authorized attacker to elevate privileges locally.	4.7	More Details
CVE-2025-11595	A vulnerability was found in Campcodes Online Apartment Visitor Management System 1.0. Impacted is an unknown function of the file /admin-profile.php. Performing manipulation of the argument mobilenumber results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-10281	BBOT's git_clone module could be abused to disclose a GitHub API key to an attacker controlled server with a malicious formatted git URL.	4.7	More Details
CVE-2025-10282	BBOT's gitlab module could be abused to disclose a GitLab API key to an attacker controlled server with a malicious formatted git URL.	4.7	More Details
CVE-2025-11167	The CM Registration – Tailored tool for seamless login and invitation-based registrations plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 2.5.6. This is due to insufficient validation on the redirect url supplied via the 'redirect_url' parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	4.7	More Details
CVE-2025-11665	A vulnerability was detected in D-Link DAP-2695 2.00RC131. This affects the function fwupdater_main of the file rgbin of the component Firmware Update Handler. Performing manipulation results in os command injection. The attack may be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2025-48464	Successful exploitation of the vulnerability could allow an unauthenticated attacker to gain access to a victim's Sync account data such as account credentials and email protection information.	4.7	More Details
CVE-2025-11470	A security vulnerability has been detected in SourceCodester Hotel and Lodge Management System up to 1.0. The impacted element is an unknown function of the file /manage_website.php. The manipulation of the argument website_image/back_login_image leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details

CVE-2025-11663	A weakness has been identified in Campcodes Online Beauty Parlor Management System 1.0. The affected element is an unknown function of the file /admin/manage-services.php. This manipulation of the argument sername causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-11664	A security vulnerability has been detected in Campcodes Online Beauty Parlor Management System 1.0. The impacted element is an unknown function of the file /admin/search-appointment.php. Such manipulation of the argument searchdata leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-11508	A security vulnerability has been detected in code-projects Voting System 1.0. This affects an unknown function of the file /admin/voters_add.php. Such manipulation of the argument photo leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-11668	A vulnerability was determined in code-projects Automated Voting System 1.0. Affected by this issue is some unknown functionality of the file /admin/update_user.php. This manipulation of the argument Password causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-10986	Path traversal in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to write data in unintended locations on disk.	4.7	More Details
CVE-2025-11628	A flaw has been found in jimit105 Project-Online-Shopping-Website up to 7d892f442bd8a96dd242dbe2b9bd5ed641e13e64. This affects an unknown function of the file /delete.php of the component Product Inventory Handler. This manipulation of the argument product_code causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-21063	Improper access control in Samsung Voice Recorder prior to version 21.5.73.12 in Android 15 and 21.5.81.40 in Android 16 allows physical attackers to access recording files on the lock screen.	4.6	More Details
CVE-2025-11570	Versions of the package drupal-pattern-lab/unified-twig-extensions from 0.0.0 are vulnerable to Cross-site Scripting (XSS) due to insufficient filtering of data. **Note:** This is exploitable only if the code is executed outside of Drupal; the function is intended to be shared between Drupal and Pattern Lab. The package drupal-pattern-lab/unified-twig-extensions is unmaintained, the fix for this issue exists in version 1.1.1 of [drupal/unified_twig_ext] (https://www.drupal.org/project/unified_twig_ext)	4.6	More Details
CVE-2025-31992	HCL Unica MaxAI Assistant is susceptible to a HTML injection vulnerability. An attacker could insert special characters that are processed client-side in the context of the user's session.	4.6	More Details
CVE-2025-11489	A security vulnerability has been detected in wonderwhy-er DesktopCommanderMCP up to 0.2.13. This vulnerability affects the function isPathAllowed of the file src/tools/filesystem.ts. The manipulation leads to symlink following. The attack can only be performed from a local environment. The attack's complexity is rated as high. It is stated that the exploitability is difficult. The exploit has been disclosed publicly and may be used. The vendor explains: "Our restriction features are designed as guardrails for LLMs to help them stay closer to what users want, rather than hardened security boundaries. (...) For users where security is a top priority, we continue to recommend using Desktop Commander with Docker, which provides actual isolation. (...) We'll keep this issue open for future consideration if we receive more user demand for improved restrictions." This vulnerability only affects products that are no longer supported by the maintainer.	4.5	More Details
CVE-2025-40774	A vulnerability has been identified in SiPass integrated (All versions < V3.0). Affected server applications store user passwords encrypted in its database. Decryption keys are accessible to users with administrative privileges, allowing them to recover passwords. Successful exploitation of this vulnerability allows an attacker to obtain and use valid user passwords. This can lead to unauthorized access to user accounts, data breaches, and potential system	4.4	More Details

	compromise.		
CVE-2025-43724	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an authorization bypass through user-controlled key vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain unauthorized access to NFSv4 or SMB shares.	4.4	More Details
CVE-2025-11635	A weakness has been identified in Tomofun Furbo 360 up to FB0035_FW_036. This vulnerability affects unknown code of the component File Upload. This manipulation causes resource consumption. Remote exploitation of the attack is possible. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-54822	An improper authorization vulnerability [CWE-285] in Fortinet FortiOS version 7.4.0 through 7.4.1 and before 7.2.8 & Fortinet FortiProxy before version 7.4.8 allows an authenticated attacker to access static files of others VDOMs via crafted HTTP or HTTPS requests.	4.3	More Details
CVE-2025-42903	A vulnerability in SAP Financial Service Claims Management RFC function ICL_USER_GET_NAME_AND_ADDRESS allows user enumeration and potential disclosure of personal data through response discrepancies, causing low impact on confidentiality with no impact on integrity or availability.	4.3	More Details
CVE-2025-11254	The Contest Gallery – Upload, Vote & Sell with PayPal and Stripe plugin for WordPress is vulnerable to CSV Injection in all versions up to, and including, 27.0.3 via gallery submissions. This makes it possible for unauthenticated attackers to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	4.3	More Details
CVE-2025-36636	In Tenable Security Center versions prior to 6.7.0, an improper access control vulnerability exists where an authenticated user could access areas outside of their authorized scope.	4.3	More Details
CVE-2025-35059	Newforma Info Exchange (NIX) '/DownloadWeb/hyperlinkredirect.aspx' provides an unauthenticated URL redirect via the 'nhl' parameter.	4.3	More Details
CVE-2025-10375	The Web Accessibility By accessiBe plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.10. This is due to missing nonce validation on multiple AJAX actions including accessibe_signup, accessibe_login, accessibe_license_trial, accessibe_modify_config, and accessibe_add_verification_page. This makes it possible for unauthenticated attackers to modify plugin settings and create verification files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-10376	The Course Redirects for Learndash plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.4. This is due to missing nonce validation when processing form submissions on the settings page. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-8682	The Newsup theme for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the newsup_admin_info_install_plugin() function in all versions up to, and including, 5.0.10. This makes it possible for unauthenticated attackers to install the ansar-import plugin.	4.3	More Details
CVE-2025-10732	The SureForms – Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to Sensitive Information Disclosure in all versions up to, and including, 1.12.1. This is due to improper access control implementation on the '/wp-json/sureforms/v1/srfm-global-settings' REST API endpoint. This makes it possible for authenticated attackers, with contributor-level access and above, to retrieve sensitive information including API keys for Google reCAPTCHA, Cloudflare Turnstile, hCaptcha, admin email addresses, and security-related form settings.	4.3	More Details
CVE-2025-42939	SAP S/4HANA (Manage Processing Rules - For Bank Statements) allows an authenticated attacker with basic privileges to delete conditions from any shared rule of any user by tampering the request parameter. Due to missing authorization check, the attacker can delete shared rule conditions that should be restricted, compromising the integrity of the application	4.3	More Details

	without affecting its confidentiality or availability.		
CVE-2025-9621	The WidgetPack Comment System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6.1. This is due to missing or incorrect nonce validation on the wpcmt_sync action in the wpcmt_request_handler function. This makes it possible for unauthenticated attackers to trigger comment synchronization events via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-9626	The Page Blocks plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing or incorrect nonce validation on the admin_process_widget_page_change function. This makes it possible for unauthenticated attackers to modify widget page block configurations via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-21055	Out-of-bounds read and write in libimagecodec.quram.so prior to SMR Oct-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-11512	A vulnerability was found in code-projects Voting System 1.0. Affected by this issue is some unknown functionality of the file /admin/voters_add.php. The manipulation of the argument Firstname/Lastname/Platform results in cross site scripting. The attack can be executed remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2025-62176	Mastodon is a free, open-source social network server based on ActivityPub. In Mastodon before 4.4.6, 4.3.14, and 4.2.27, the streaming server accepts serving events for public timelines to clients using any valid authentication token, even if those tokens lack the read:statuses scope. This allows OAuth clients without the read scope to subscribe to public channels and receive public timeline events. The impact is limited, as this only affects new public posts published on the public timelines and requires an otherwise valid token, but this may lead to unexpected access to public posts in a limited-federation setting. This issue has been patched in versions 4.4.6, 4.3.14, and 4.2.27. No known workarounds exist.	4.3	More Details
CVE-2025-62175	Mastodon is a free, open-source social network server based on ActivityPub. In versions before 4.4.6, 4.3.14, and 4.2.27, disabling or suspending a user account does not disconnect the account from the streaming API. This allows disabled or suspended accounts to continue receiving real-time updates through existing streaming connections and to establish new streaming connections, even though they cannot interact with other API endpoints. This undermines moderation actions, as administrators expect disabled or suspended accounts to be fully disconnected from the service. This issue has been patched in versions 4.4.6, 4.3.14, and 4.2.27. No known workarounds exist.	4.3	More Details
CVE-2025-2934	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 5.2 prior to 18.2.8, 18.3 prior to 18.3.4, and 18.4 prior to 18.4.2 that could have allowed an authenticated attacker to create a denial of service condition by configuring malicious webhook endpoints that send crafted HTTP responses.	4.3	More Details
CVE-2025-61996	OPEXUS FOIAXpress before 11.13.3.0 allows an administrative user to inject JavaScript or other content within the Annual Report Template. Injected content is executed in the context of other users when they generate an Annual Report. Successful exploitation allows the administrative user to perform actions on behalf of the target, including stealing session cookies, user credentials, or sensitive data.	4.3	More Details
CVE-2025-11637	A vulnerability was detected in Tomofun Furbo 360 up to FB0035_FW_036. Impacted is an unknown function of the component Audio Handler. Performing manipulation results in race condition. The attack is possible to be carried out remotely. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-11638	A flaw has been found in Tomofun Furbo 360 and Furbo Mini. The affected element is an unknown function of the component Bluetooth Handler. Executing manipulation can lead to denial of service. The attacker needs to be present on the local network. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE-2025-36225	IBM Aspera 5.0.0 through 5.0.13.1 could disclose sensitive user information from the system to an authenticated user due to an observable discrepancy of returned data.	4.3	More Details
CVE-2025-31994	HCL Unica Campaign 12.1.10 is vulnerable to Reflected Cross-Site Scripting (XSS) where an attacker injects malicious script into an HTTP request, which is then reflected unsafely in the server's immediate response to the victim's browser, executing the script as if it originated from the trusted website.	4.3	More Details
CVE-2025-11618	A missing validation check in FreeRTOS-Plus-TCP's UDP/IPv6 packet processing code can lead to an invalid pointer dereference when receiving a UDP/IPv6 packet with an incorrect IP version field in the packet header. This issue only affects applications using IPv6. We recommend upgrading to the latest version and ensure any forked or derivative code is patched to incorporate the new fixes.	4.3	More Details
CVE-2025-61906	Opencast is a free, open-source platform to support the management of educational audio and video content. Prior to Opencast 17.8 and 18.2, in some situations, Opencast's editor may publish a video without notifying the user. This may lead to users accidentally publishing media not meant for publishing, and thus possibly exposing internal media. This risk of this actually impacting someone is very low, though. This can only be triggered by users with write access to an event. They also have to use the editor, which is usually an action taken if they want to publish media and not something users would use on internal media they do not want to publish. Finally, they have to first click on "Save & Publish" before then selecting the "Save" option. Nevertheless, while very unlikely, this can happen. This issue is fixed in Opencast 17.8 and 18.2.	4.3	More Details
CVE-2025-61997	OPEXUS FOIAXpress before 11.13.3.0 allows an administrative user to inject JavaScript or other content within the Annual Report Enterprise Banner image upload field. Injected content is executed in the context of other users when they generate an Annual Report. Successful exploitation allows the administrative user to perform actions on behalf of the target, including stealing session cookies, user credentials, or sensitive data.	4.3	More Details
CVE-2025-11442	A security flaw has been discovered in JhumanJ OpnForm up to 1.9.3. The impacted element is an unknown function of the component API Endpoint. The manipulation results in cross-site request forgery. The attack may be performed from remote. The exploit has been released to the public and may be exploited. The vendor has stated that API calls require authentication through Authorization Bearer Tokens, so classic CSRF attacks do not apply here. An attacker would need to possess the JWT through means such as XSS which were mitigated, disabling any form of initial access.	4.3	More Details
CVE-2025-61999	OPEXUS FOIAXpress before 11.13.3.0 allows an administrative user to upload JavaScript or other content embedded in an SVG image used as a logo. Injected content is executed in the context of other users when they view affected pages. Successful exploitation allows the administrative user to perform actions on behalf of the target, including stealing session cookies, user credentials, or sensitive data.	4.3	More Details
CVE-2025-11435	A security vulnerability has been detected in JhumanJ OpnForm up to 1.9.3. Affected by this vulnerability is an unknown functionality of the file /show/submissions. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The identifier of the patch is a2af1184e53953afa8cb052f4055f288adcaa608. To fix this issue, it is recommended to deploy a patch.	4.3	More Details
CVE-2025-11439	A vulnerability was found in JhumanJ OpnForm up to 1.9.3. This issue affects some unknown processing of the file /show/integrations. Performing manipulation results in missing authorization. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The patch is named 11d97d78f2de2cb49f79baed6bde8b611ec1f384. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2025-11440	A vulnerability was determined in JhumanJ OpnForm up to 1.9.3. Impacted is an unknown function of the file /edit. Executing manipulation can lead to improper access controls. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This patch is called b15e29021d326be127193a5dbbd528c4e37e6324. Applying a patch is advised to resolve this issue.	4.3	More Details

CVE-2024-47569	A insertion of sensitive information into sent data in Fortinet FortiManager Cloud 7.4.1 through 7.4.3, FortiVoice 7.0.0 through 7.0.4, 6.4.0 through 6.4.9, 6.0.7 through 6.0.12, FortiMail 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.9, FortiOS 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.8, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15, 6.2.0 through 6.2.17, 6.0.0 through 6.0.18, FortiWeb 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.11, 7.0.0 through 7.0.11, 6.4.0 through 6.4.3, FortiRecorder 7.2.0 through 7.2.1, 7.0.0 through 7.0.4, FortiNDR 7.6.0 through 7.6.1, 7.4.0 through 7.4.8, 7.2.0 through 7.2.5, 7.1.0 through 7.1.1, 7.0.0 through 7.0.7, 1.5.0 through 1.5.3, FortiPAM 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiTester 7.4.0 through 7.4.2, 7.3.0 through 7.3.2, 7.2.0 through 7.2.3, 7.1.0 through 7.1.1, 7.0.0, 4.2.0 through 4.2.1, FortiProxy 7.4.0 through 7.4.4, 7.2.0 through 7.2.10, 7.0.0 through 7.0.21, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiManager 7.6.0 through 7.6.1, 7.4.1 through 7.4.3 allows attacker to disclose sensitive information via specially crafted packets.	4.3	More Details
CVE-2025-62292	In SonarQube before 25.6, 2025.3 Commercial, and 2025.1.3 LTA, authenticated low-privileged users can query the /api/v2/users-management/users endpoint and obtain user fields intended for administrators only, including the email addresses of other accounts.	4.3	More Details
CVE-2025-61998	OPEXUS FOIAXpress before 11.13.3.0 allows an administrative user to inject JavaScript or other content as a URL within the Technical Support Hyperlink Manager. Injected content is executed in the context of other users when they click the malicious link. Successful exploitation allows the administrative user to perform actions on behalf of the target, including stealing session cookies, user credentials, or sensitive data.	4.3	More Details
CVE-2025-31997	HCL Unica Centralized Offer Management is vulnerable to Insecure Direct Object References (IDOR). An attacker can bypass authorization and access resources in the system directly, for example database records or files.	4.2	More Details
CVE-2025-60308	code-projects Simple Online Hotel Reservation System 1.0 has a Cross Site Scripting (XSS) vulnerability in the Add Room function of the online hotel reservation system. Malicious JavaScript code is entered in the Description field, which can leak the administrator's cookie information when browsing this room information	4.1	More Details
CVE-2025-21070	Out-of-bounds write in the SPI decoder in Samsung Notes prior to version 4.4.30.63 allows local attackers to write out-of-bounds memory.	4.0	More Details
CVE-2025-21069	Out-of-bounds read in the parsing of image data in Samsung Notes prior to version 4.4.30.63 allows local attackers to access out-of-bounds memory.	4.0	More Details
CVE-2025-31969	HCL Unica Platform is impacted by misconfigured Content Security Policy (CSP). These can result in malicious resources getting loaded and browsers may come across certain types of attacks, such as cross-site scripting and clickjacking.	4.0	More Details
CVE-2025-21057	Use of implicit intent for sensitive communication in Samsung Notes prior to version 4.4.30.63 allows local attackers to access shared notes.	4.0	More Details
CVE-2025-21052	Out-of-bounds write under specific condition in the pre-processing of JPEG decoding in libpadm.so prior to SMR Oct-2025 Release 1 allows local attackers to cause memory corruption.	4.0	More Details
CVE-2025-21053	Out-of-bounds write in the parsing header for JPEG decoding in libpadm.so prior to SMR Oct-2025 Release 1 allows local attackers to cause memory corruption.	4.0	More Details
CVE-2025-21066	Out-of-bounds read in the SPI decoder in Samsung Notes prior to version 4.4.30.63 allows local attackers to access out-of-bounds memory.	4.0	More Details
CVE-2025-21068	Out-of-bounds read in the reading of image data in Samsung Notes prior to version 4.4.30.63 allows local attackers to access out-of-bounds memory.	4.0	More Details

CVE-2025-58277	Permission verification bypass vulnerability in the Camera app. Successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-2025-21067	Out-of-bounds read in the allocation of image buffer in Samsung Notes prior to version 4.4.30.63 allows local attackers to access out-of-bounds memory.	4.0	More Details
CVE-2025-21045	Insecure storage of sensitive information in Galaxy Watch prior to SMR Oct-2025 Release 1 allows local attackers to access sensitive information.	4.0	More Details
CVE-2025-21051	Out-of-bounds write in the pre-processing of JPEG decoding in libpadm.so prior to SMR Oct-2025 Release 1 allows local attackers to write out-of-bounds memory.	4.0	More Details
CVE-2025-11642	A vulnerability was identified in Tomofun Furbo 360 and Furbo Mini. Affected is an unknown function of the component Registration Handler. Such manipulation leads to denial of service. The attack can be executed directly on the physical device. The attack requires a high level of complexity. The exploitability is told to be difficult. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	4.0	More Details
CVE-2025-21054	Out-of-bounds read in the parsing header for JPEG decoding in libpadm.so prior to SMR Oct-2025 Release 1 allows local attackers to potentially access out-of-bounds memory.	4.0	More Details
CVE-2025-11641	A vulnerability was determined in Tomofun Furbo 360 and Furbo Mini. This impacts an unknown function of the component Trial Restriction Handler. This manipulation causes improper access controls. It is feasible to perform the attack on the physical device. The attack is considered to have high complexity. The exploitability is said to be difficult. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	3.9	More Details
CVE-2025-8594	The Pz-LinkCard WordPress plugin before 2.5.7 does not validate a parameter before making a request to it, which could allow users with a role as low as Contributor to perform SSRF attack.	3.8	More Details
CVE-2025-52630	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in HCL AION.This issue affects AION: 2.0.	3.7	More Details
CVE-2025-52634	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in HCL AION This issue affects HCL AION: 2.0.	3.7	More Details
CVE-2025-52625	A vulnerability Cacheable SSL Page Found vulnerability has been identified in HCL AION. Cached data may expose credentials, system identifiers, or internal file paths to attackers with access to the device or browser This issue affects AION: 2.0.	3.7	More Details
CVE-2025-11643	A security flaw has been discovered in Tomofun Furbo 360 and Furbo Mini. Affected by this vulnerability is an unknown functionality of the file /squashfs-root/furbo_img of the component MQTT Client Certificate. Performing manipulation results in hard-coded credentials. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitation appears to be difficult. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-11633	A vulnerability was identified in Tomofun Furbo 360 and Furbo Mini. Affected by this issue is the function upload_file_to_s3 of the file collect_logs.sh of the component HTTP Traffic Handler. The manipulation leads to improper certificate validation. The attack may be initiated remotely. The attack is considered to have high complexity. The exploitation is known to be difficult. The firmware versions determined to be affected are Furbo 360 up to	3.7	More Details

	FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-11609	A flaw has been found in code-projects Hospital Management System 1.0. Affected is the function session of the component express-session. This manipulation of the argument secret with the input secret causes use of hard-coded cryptographic key . The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is told to be difficult. The exploit has been published and may be used.	3.7	More Details
CVE-2025-11443	A weakness has been identified in JhumanJ OpnForm up to 1.9.3. This affects an unknown function of the file /api/password/email of the component Forgotten Password Handler. This manipulation causes information exposure through discrepancy. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is reported as difficult. The exploit has been made available to the public and could be exploited. This issue is currently aligned with Laravel issue #46465, which is why no mitigation action was taken.	3.7	More Details
CVE-2025-11441	A vulnerability was identified in JhumanJ OpnForm up to 1.9.3. The affected element is an unknown function of the component HTTP Header Handler. The manipulation of the argument X-Forwarded-For leads to improper restriction of excessive authentication attempts. The attack is possible to be carried out remotely. A high degree of complexity is needed for the attack. The exploitability is described as difficult. The exploit is publicly available and might be used. The identifier of the patch is 11e99960e14ca986b1a001a56e7533223d2cfa5b. It is suggested to install a patch to address this issue.	3.7	More Details
CVE-2025-52635	A rusted types in scripts not enforced in CSP vulnerability has been identified in HCL AION.This issue affects AION: 2.0.	3.7	More Details
CVE-2025-62178	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.1, a Reflected Cross-Site Scripting (XSS) vulnerability was identified in the /html/atendido/cadastro_atendido_parentesco_pessoa_nova.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the idatendido parameter. This vulnerability is fixed in 3.5.1.	3.5	More Details
CVE-2025-2138	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user on the network to delete comments from other users due to client-side enforcement of server-side security.	3.5	More Details
CVE-2025-40773	A vulnerability has been identified in SiPass integrated (All versions < V3.0). Affected server applications contains a broken access control vulnerability. The authorization mechanism lacks sufficient server-side checks, allowing an attacker to execute a specific API request. Successful exploitation allows an attacker to potentially manipulate data belonging to other users.	3.5	More Details
CVE-2025-2139	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user on the network to delete reviews from other users due to client-side enforcement of server-side security.	3.5	More Details
CVE-2025-52614	HCL Unica Platform is affected by a Cookie without HTTPOnly Flag Set vulnerability. A malicious agent may be able to induce this event by feeding a user suitable links, either directly or via another web site.	3.5	More Details
CVE-2025-58084	Mattermost Desktop App versions <= 5.13.0 fail to validate URLs external to the configured Mattermost servers, allowing an attacker on a server the user has configured to crash the user's application by sending the user a malformed URL.	3.5	More Details
CVE-2025-11433	A security flaw has been discovered in itsourcecode Leave Management System 1.0. This impacts the function redirect of the file /module/employee/controller.php?action=reset of the component Query Parameter Handler. Performing manipulation of the argument ID results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	3.5	More Details
CVE-	A flaw has been found in code-projects Voting System 1.0. The affected element is an unknown function of the file /admin/candidates_edit.php. This manipulation of the argument		More

2025-11421	Firstname/Lastname/Platform causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used.	3.5	Details
CVE-2025-62174	Mastodon is a free, open-source social network server based on ActivityPub. In Mastodon before 4.4.6, 4.3.14, and 4.2.27, when an administrator resets a user account's password via the command-line interface using `bin/tootctl accounts modify --reset-password`, active sessions and access tokens for that account are not revoked. This allows an attacker with access to a previously compromised session or token to continue using the account after the password has been reset. This issue has been patched in versions 4.2.27, 4.3.14, and 4.4.6. No known workarounds exist.	3.5	More Details
CVE-2025-31993	HCL Unica Centralized Offer Management is vulnerable to a potential Server-Side Request Forgery (SSRF). An attacker can exploit improper input validation by submitting maliciously crafted input to a target application running on a server.	3.5	More Details
CVE-2025-31998	HCL Unica Centralized Offer Management is vulnerable to poor unhandled exceptions which exposes sensitive information. An attacker can exploit use this information to exploit known vulnerabilities launch targeted attacks, such as remote code execution or denial of service.	3.5	More Details
CVE-2025-52615	HCL Unica Platform is impacted by misconfigured security related HTTP headers. This can lead to less secure browser default treatment for the policies controlled by these headers.	3.5	More Details
CVE-2025-31995	HCL Unica MaxAI Workbench is vulnerable to improper input validation. This allows attackers to exploit vulnerabilities such as SQL Injection, XSS, or command injection, leading to unauthorized access or data breaches, etc.	3.5	More Details
CVE-2025-58292	Denial of service (DoS) vulnerability in the office service. Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-11639	A vulnerability has been found in Tomofun Furbo 360 and Furbo Mini. The impacted element is an unknown function of the file collect_logs.sh of the component Debug Log S3 Bucket Handler. The manipulation leads to insecure storage of sensitive information. An attack has to be approached locally. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2025-58291	Denial of service (DoS) vulnerability in the office service. Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-58290	Denial of service (DoS) vulnerability in the office service. Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-58286	Denial of service (DoS) vulnerability in the office service. Successful exploitation of this vulnerability may affect availability.	3.3	More Details
CVE-2025-59284	Exposure of sensitive information to an unauthorized actor in Windows NTLM allows an unauthorized attacker to perform spoofing locally.	3.3	More Details
CVE-2025-11494	A vulnerability was found in GNU Binutils 2.45. Impacted is the function _bfd_x86_elf_late_size_sections of the file bfd/elfxx-x86.c of the component Linker. The manipulation results in out-of-bounds read. The attack needs to be approached locally. The exploit has been made public and could be used. The patch is identified as b6ac5a8a5b82f0ae6a4642c8d7149b325f4cc60a. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2025-11495	A vulnerability was determined in GNU Binutils 2.45. The affected element is the function elf_x86_64_relocate_section of the file elf64-x86-64.c of the component Linker. This manipulation causes heap-based buffer overflow. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. Patch name:	3.3	More Details

	6b21c8b2ecfef5c95142cbc2c32f185cb1c26ab0. To fix this issue, it is recommended to deploy a patch.		
CVE-2025-61786	Deno is a JavaScript, TypeScript, and WebAssembly runtime. In versions prior to 2.5.3 and 2.2.15, `Deno.FsFile.prototype.stat` and `Deno.FsFile.prototype.statSync` are not limited by the permission model check `--deny-read=./`. It's possible to retrieve stats from files that the user do not have explicit read access to (the script is executed with `--deny-read=./`). Similar APIs like `Deno.stat` and `Deno.statSync` require `allow-read` permission, however, when a file is opened, even with file-write only flags and deny-read permission, it's still possible to retrieve file stats, and thus bypass the permission model. Versions 2.5.3 and 2.2.15 fix the issue.	3.3	More Details
CVE-2025-59280	Improper authentication in Windows SMB Client allows an unauthorized attacker to perform tampering over a network.	3.1	More Details
CVE-2025-11640	A vulnerability was found in Tomofun Furbo 360 and Furbo Mini. This affects an unknown function of the component Bluetooth Low Energy. The manipulation results in cleartext transmission of sensitive information. Access to the local network is required for this attack. Attacks of this nature are highly complex. The exploitability is reported as difficult. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-54196	Adobe Connect versions 12.9 and earlier are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. An attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction in that a victim must click on a crafted link.	3.1	More Details
CVE-2025-52655	Inclusion of Functionality from Untrusted Control Sphere vulnerability in HCL MyXalytics. v6.6 allows Loading third-party scripts without integrity checks or validation can allow external code run in the application's context, risking data exposure.	3.1	More Details
CVE-2025-11647	A flaw has been found in Tomofun Furbo 360 and Furbo Mini. This issue affects some unknown processing of the component GATT Service. This manipulation of the argument DeviceToken causes information disclosure. The attack is only possible within the local network. A high degree of complexity is needed for the attack. The exploitability is assessed as difficult. The exploit has been published and may be used. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-11731	A flaw was found in the exsltFuncResultComp() function of libxslt, which handles EXSLT <func:result> elements during stylesheet parsing. Due to improper type handling, the function may treat an XML document node as a regular XML element node, resulting in a type confusion. This can cause unexpected memory reads and potential crashes. While difficult to exploit, the flaw could lead to application instability or denial of service.	3.1	More Details
CVE-2025-42909	SAP Cloud Appliance Library Appliances allows an attacker with high privileges to leverage an insecure S/4HANA default profile setting in an existing SAP CAL appliances to gain access to other appliances. This has low impact on confidentiality of the application, integrity and availability is not impacted.	3.0	More Details
CVE-2025-58282	Permission control vulnerability in the camera module. Successful exploitation of this vulnerability may affect service confidentiality.	2.8	More Details
CVE-2025-31514	An Insertion of Sensitive Information into Log File vulnerability [CWE-532] in FortiOS 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow an attacker with at least read-only privileges to retrieve sensitive 2FA-related information via observing logs or via diagnose command.	2.7	More Details
CVE-2025-58903	An Unchecked Return Value vulnerability [CWE-252] in Fortinet FortiOS version 7.6.0 through 7.6.3 and before 7.4.8 API allows an authenticated user to cause a Null Pointer Dereference, crashing the http daemon via a specialy crafted request.	2.7	More Details

CVE-2025-47890	An URL Redirection to Untrusted Site vulnerabilities [CWE-601] in FortiOS 7.6.0 through 7.6.2, 7.4.0 through 7.4.8, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiProxy 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0 all versions; FortiSASE 25.2.a may allow an unauthenticated attacker to perform an open redirect attack via crafted HTTP requests.	2.6	More Details
CVE-2025-11437	A flaw has been found in JhumanJ OpnForm up to 1.9.3. This affects an unknown part of the file /api/open/forms/ of the component Form Editor. This manipulation causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used. This issue is currently under review for additional handling. As of right now the vendor has stated that the feature is disabled until the user has configured their own domain which will mitigate this attack vector.	2.4	More Details
CVE-2025-11425	A vulnerability was identified in projectworlds Advanced Library Management System 1.0. Affected is an unknown function of the file /edit_admin.php. The manipulation of the argument firstname leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. Other parameters might be affected as well.	2.4	More Details
CVE-2025-11634	A security flaw has been discovered in Tomofun Furbo 360 and Furbo Mini. This affects an unknown part of the component UART Interface. The manipulation results in information disclosure. An attack on the physical device is feasible. The exploit has been released to the public and may be exploited. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-11485	A vulnerability was determined in SourceCodester Student Grades Management System 1.0. Affected is the function add_user of the file /admin.php of the component Manage Users Page. This manipulation of the argument first_name/last_name causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-2025-11645	A security vulnerability has been detected in Tomofun Furbo Mobile App up to 7.57.0a on Android. This affects an unknown part of the component Authentication Token Handler. The manipulation leads to insecure storage of sensitive information. It is possible to launch the attack on the physical device. 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-2025-8606	The GSheetConnector For Gravity Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions less than, or equal to, 1.3.23. This is due to missing or incorrect nonce validation on the activate_plugin and deactivate_plugin functions. This makes it possible for attackers to trick authenticated administrators into activating or deactivating specified plugins via a forged request, such as clicking on a malicious link or visiting a compromised page.	2.4	More Details
CVE-2025-21046	Improper access control in WindowManager in Samsung DeX prior to SMR Oct-2025 Release 1 allows physical attackers to temporarily access to recent app list.	2.4	More Details
CVE-2025-59294	Exposure of sensitive information to an unauthorized actor in Windows Taskbar Live allows an unauthorized attacker to disclose information with a physical attack.	2.1	More Details
CVE-2025-11644	A weakness has been identified in Tomofun Furbo 360 and Furbo Mini. Affected by this issue is some unknown functionality of the component UART Interface. Executing manipulation can lead to insecure storage of sensitive information. The physical device can be targeted for the attack. This attack is characterized by high complexity. The exploitation is known to be difficult. The exploit has been made available to the public and could be exploited. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.	2.0	More Details
CVE-2025-11650	A vulnerability was determined in Tomofun Furbo 360 and Furbo Mini. The impacted element is an unknown function of the file /etc/shadow of the component Password Handler. Executing manipulation can lead to use of weak hash. The physical device can be targeted for the attack. The attack requires a high level of complexity. The exploitability is regarded as difficult. The exploit has been publicly disclosed and may be utilized. The firmware versions determined to be affected are Furbo 360 up to FB0035_FW_036 and Furbo Mini up to	1.8	More Details

	MC0020_FW_074. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-62240	Multiple cross-site scripting (XSS) vulnerabilities with Calendar events in Liferay Portal 7.4.3.35 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.7, 7.4 update 35 through update 92, and 7.3 update 25 through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user’s (1) First Name, (2) Middle Name or (3) Last Name text field.	N/A	More Details
CVE-2025-61785	Deno is a JavaScript, TypeScript, and WebAssembly runtime. In versions prior to 2.5.3 and 2.2.15, `Deno.FsFile.prototype.utime` and `Deno.FsFile.prototype.utimeSync` are not limited by the permission model check `--deny-write=./`. It's possible to change to change the access (`atime`) and modification (`mtime`) times on the file stream resource even when the file is opened with `read` only permission (and `write`: `false`) and file write operations are not allowed (the script is executed with `--deny-write=./`). Similar APIs like `Deno.utime` and `Deno.utimeSync` require `allow-write` permission, however, when a file is opened, even with read only flags and deny-write permission, it's still possible to change the access (`atime`) and modification (`mtime`) times, and thus bypass the permission model. Versions 2.5.3 and 2.2.15 fix the issue.	N/A	More Details
CVE-2025-61926	Allstar is a GitHub App to set and enforce security policies. In versions prior to 4.5, a vulnerability in Allstar’s Reviewbot component caused inbound webhook requests to be validated against a hard-coded, shared secret. The value used for the secret token was compiled into the Allstar binary and could not be configured at runtime. In practice, this meant that every deployment using Reviewbot would validate requests with the same secret unless the operator modified source code and rebuilt the component - an expectation that is not documented and is easy to miss. All Allstar releases prior to v4.5 that include the Reviewbot code path are affected. Deployments on v4.5 and later are not affected. Those who have not enabled or exposed the Reviewbot endpoint are not exposed to this issue.	N/A	More Details
CVE-2025-61928	Better Auth is an authentication and authorization library for TypeScript. In versions prior to 1.3.26, unauthenticated attackers can create or modify API keys for any user by passing that user's id in the request body to the `api/auth/api-key/create` route. `session?.user ?? (authRequired ? null : { id: ctx.body.userId })`. When no session exists but `userId` is present in the request body, `authRequired` becomes false and the user object is set to the attacker-controlled ID. Server-only field validation only executes when `authRequired` is true (lines 280-295), allowing attackers to set privileged fields. No additional authentication occurs before the database operation, so the malicious payload is accepted. The same pattern exists in the update endpoint. This is a critical authentication bypass enabling full an unauthenticated attacker can generate an API key for any user and immediately gain complete authenticated access. This allows the attacker to perform any action as the victim user using the api key, potentially compromise the user data and the application depending on the victim's privileges. Version 1.3.26 contains a patch for the issue.	N/A	More Details
CVE-2025-11449	ServiceNow has addressed a reflected cross-site scripting vulnerability that was identified in the ServiceNow AI Platform. This vulnerability could result in arbitrary code being executed within the browsers of ServiceNow users who click on a specially crafted link. ServiceNow has addressed this vulnerability by deploying a relevant security update to the majority of hosted instances. Relevant security updates also have been provided to ServiceNow self-hosted customers, partners, and hosted customers with unique configuration. Further, the vulnerability is addressed in the listed patches and hot fixes. We recommend customers promptly apply appropriate updates or upgrade if they have not already done so.	N/A	More Details
CVE-2025-11450	ServiceNow has addressed a reflected cross-site scripting vulnerability that was identified in the ServiceNow AI Platform. This vulnerability could result in arbitrary code being executed within the browsers of ServiceNow users who click on a specially crafted link. ServiceNow has addressed this vulnerability by deploying a relevant security update to the majority of hosted instances. Relevant security updates also have been provided to ServiceNow self-hosted customers, partners, and hosted customers with unique configurations. Further, the vulnerability is addressed in the listed patches and hot fixes. We recommend customers promptly apply appropriate updates or upgrade if they have not already done so.	N/A	More Details
CVE-	Stored cross-site scripting (XSS) vulnerability in Forms in Liferay Portal 7.3.2 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4		

2025-43830	GA through update 92, and 7.3 GA through update 35 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a form with a rich text type field.	N/A	More Details
CVE-2025-61871	NAS Navigator2 Windows version by BUFFALO INC. registers a Windows service with an unquoted file path. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2025-10351	SQL injection vulnerability based on the melis-cms module of the Melis platform from Melis Technology. This vulnerability allows an attacker to retrieve, create, update, and delete databases through the 'idPage' parameter in the '/melis/MelisCms/PageEdition/getTinyTemplates' endpoint.	N/A	More Details
CVE-2025-59051	The FreePBX Endpoint Manager module includes a Network Scanning feature that provides web-based access to nmap functionality for network device discovery. In Endpoint Manager 16 before 16.0.92 and 17 before 17.0.6, insufficiently sanitized user-supplied input allows authenticated OS command execution as the asterisk user. Authentication with a known username is required. Updating to Endpoint Manager 16.0.92 or 17.0.6 addresses the issue.	N/A	More Details
CVE-2025-59429	FreePBX is an open source GUI for managing Asterisk. In versions prior to 16.0.68.39 for FreePBX 16 and versions prior to 17.0.18.38 for FreePBX 17, a reflected cross-site scripting vulnerability is present on the Asterisk HTTP Status page. The Asterisk HTTP status page is exposed by FreePBX and is available by default on version 16 via any bound IP address at port 8088. By default on version 17, the binding is only to localhost IP, making it significantly less vulnerable. The vulnerability can be exploited by unauthenticated attackers to obtain cookies from logged-in users, allowing them to hijack a session of an administrative user. The theft of admin session cookies allows attackers to gain control over the FreePBX admin interface, enabling them to access sensitive data, modify system configurations, create backdoor accounts, and cause service disruption. This issue has been patched in version 16.0.68.39 for FreePBX 16 and version 17.0.18.38 for FreePBX 17.	N/A	More Details
CVE-2025-60374	Stored Cross-Site Scripting (XSS) in Perfex CRM chatbot before 3.3.1 allows attackers to inject arbitrary HTML/JavaScript. The payload is executed in the browsers of users viewing the chat, resulting in client-side code execution, potential session token theft, and other malicious actions. A different vulnerability than CVE-2024-8867.	N/A	More Details
CVE-2025-60540	karakeep v0.26.0 to v0.7.0 was discovered to contain a Server-Side Request Forgery (SSRF).	N/A	More Details
CVE-2025-61675	FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. In versions prior to 16.0.92 for FreePBX 16 and versions prior to 17.0.6 for FreePBX 17, the Endpoint Manager module contains authenticated SQL injection vulnerabilities affecting multiple parameters in the basestation, model, firmware, and custom extension configuration functionality areas. Authentication with a known username is required to exploit these vulnerabilities. Successful exploitation allows authenticated users to execute arbitrary SQL queries against the database, potentially enabling access to sensitive data or modification of database contents. This issue has been patched in version 16.0.92 for FreePBX 16 and version 17.0.6 for FreePBX 17.	N/A	More Details
CVE-2025-61783	Python Social Auth is a social authentication/registration mechanism. In versions prior to 5.6.0, upon authentication, the user could be associated by e-mail even if the `associate_by_email` pipeline was not included. This could lead to account compromise when a third-party authentication service does not validate provided e-mail addresses or doesn't require unique e-mail addresses. Version 5.6.0 contains a patch. As a workaround, review the authentication service policy on e-mail addresses; many will not allow exploiting this vulnerability.	N/A	More Details
CVE-2025-43829	Stored cross-site scripting (XSS) vulnerability in diagram type products in Commerce in Liferay Portal 7.4.3.18 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 18 through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a SVG file.	N/A	More Details
CVE-	Cross-site scripting (XSS) vulnerability in the Commerce Product Comparison Table widget in Liferay Portal 7.4.0 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5,		

2025-43821	2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Commerce Product's Name text field.	N/A	More Details
CVE-2025-10353	File upload leading to remote code execution (RCE) in the “melis-cms-slider” module of Melis Technology's Melis Platform. This vulnerability allows an attacker to upload a malicious file via a POST request to '/melis/MelisCmsSlider/MelisCmsSliderDetails/saveDetailsForm' using the 'mcsdetail_img' parameter.	N/A	More Details
CVE-2025-10352	Vulnerability in the melis-core module of Melis Technology's Melis Platform, which, if exploited, allows an unauthenticated attacker to create an administrator account via a request to '/melis/MelisCore/ToolUser/addNewUser'.	N/A	More Details
CVE-2025-61678	FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. In versions prior to 16.0.92 for FreePBX 16 and versions prior to 17.0.6 for FreePBX 17, the Endpoint Manager module contains an authenticated arbitrary file upload vulnerability affecting the fwbrand parameter. The fwbrand parameter allows an attacker to change the file path. Combined, these issues can result in a webshell being uploaded. Authentication with a known username is required to exploit this vulnerability. Successful exploitation allows authenticated users to upload arbitrary files to attacker-controlled paths on the server, potentially leading to remote code execution. This issue has been patched in version 16.0.92 for FreePBX 16 and version 17.0.6 for FreePBX 17.	N/A	More Details
CVE-2025-9868	Server-Side Request Forgery (SSRF) in the Remote Browser Plugin in Sonatype Nexus Repository 2.x up to and including 2.15.2 allows unauthenticated remote attackers to exfiltrate proxy repository credentials via crafted HTTP requests.	N/A	More Details
CVE-2025-61779	Confidential Containers's Trustee project contains tools and components for attesting confidential guests and providing secrets to them. In versions prior to 0.15.0, the attestation-policy endpoint didn't check if the kbs-client submitting the request was actually authenticated (had the right key). This allowed any kbs-client to actually change the attestation policy. Version 0.15.0 fixes the issue.	N/A	More Details
CVE-2025-43771	Multiple cross-site scripting (XSS) vulnerabilities in the Notifications widget in Liferay Portal 7.4.3.102 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5 and 2023.Q3.1 through 2023.Q3.10 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into (1) a user’s “First Name” text field, (2) a user’s “Middle Name” text field, (3) a user’s “Last Name” text field, (4) the “Other Reason” text field when flagging content, or (5) the name of the flagged content.	N/A	More Details
CVE-2016-15047	AVTECH devices that include the CloudSetup.cgi management endpoint are vulnerable to authenticated OS command injection. The `exefile` parameter in CloudSetup.cgi is passed to the underlying system command execution without proper validation or whitelisting. An authenticated attacker who can invoke this endpoint can supply crafted input to execute arbitrary system commands as root. Successful exploitation grants full control of the device, and - depending on deployment and whether the device stores credentials or has network reachability to internal systems - may enable credential theft, lateral movement, or data exfiltration. The archived SEARCH-LAB disclosure implies that this vulnerability was remediated in early 2017, but AVTECH has not defined an affected version range.	N/A	More Details
CVE-2025-34248	D-Link Nuclias Connect firmware versions < 1.3.1.4 contain a directory traversal vulnerability within /api/web/dnc/global/database/deleteBackup due to improper sanitization of the deleteBackupList parameter. This can allow an authenticated attacker to delete arbitrary files impacting the integrity and availability of the system.	N/A	More Details
CVE-2025-4614	An information disclosure vulnerability in Palo Alto Networks PAN-OS® software enables an authenticated administrator to view session tokens of users authenticated to the firewall web UI. This may allow impersonation of users whose session tokens are leaked. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators. Cloud NGFW and Prisma® Access are not affected by this vulnerability.	N/A	More Details
	NetSarang Xmanager Enterprise 5.0 Build 1232, Xmanager 5.0 Build 1045, Xshell 5.0 Build 1322, Xftp 5.0 Build 1218, and Xlpd 5.0 Build 1220 contain a malicious nssock2.dll that implements a multi-stage, DNS-based backdoor. The dormant library contacts a C2 DNS		

CVE-2017-20203	server via a specially crafted TXT record for a month-generated domain. After receiving a decryption key, it then downloads and executes arbitrary code, creates an encrypted virtual file system (VFS) in the registry, and grants the attacker full remote code execution, data exfiltration, and persistence. NetSarang released builds for each product line that remediated the compromise: Xmanager Enterprise Build 1236, Xmanager Build 1049, Xshell Build 1326, Xftp Build 1222, and Xlpd Build 1224. Kaspersky Lab identified an instance of exploitation in the wild in August 2017.	N/A	More Details
CVE-2025-39664	Insufficient escaping in the report scheduler within Checkmk <2.4.0p13, <2.3.0p38, <2.2.0p46 and 2.1.0 (EOL) allows authenticated attackers to define the storage location of report file pairs beyond their intended root directory.	N/A	More Details
CVE-2025-32919	Use of an insecure temporary directory in the Windows License plugin for the Checkmk Windows Agent allows Privilege Escalation. This issue affects Checkmk: from 2.4.0 before 2.4.0p13, from 2.3.0 before 2.3.0p38, from 2.2.0 before 2.2.0p46, and all versions of 2.1.0 (EOL).	N/A	More Details
CVE-2025-32916	Potential use of sensitive information in GET requests in Checkmk GmbH's Checkmk versions <2.4.0p13, <2.3.0p38, <2.2.0p46, and 2.1.0 (EOL) may cause sensitive form data to be included in URL query parameters, which may be logged in various places such as browser history or web server logs.	N/A	More Details
CVE-2025-62228	Apache Flink CDC version 3.4.0 was vulnerable to a SQL injection via maliciously crafted identifiers eg. crafted database name or crafted table name. Even through only the logged-in database user can trigger the attack, we recommend users update Flink CDC version to 3.5.0 which address this issue.	N/A	More Details
CVE-2025-39963	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix incorrect io_kiocb reference in io_link_skb In io_link_skb function, there is a bug where prev_notif is incorrectly assigned using 'nd' instead of 'prev_nd'. This causes the context validation check to compare the current notification with itself instead of comparing it with the previous notification. Fix by using the correct prev_nd parameter when obtaining prev_notif.	N/A	More Details
CVE-2025-39962	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix untrusted unsigned subtract Fix the following Smatch static checker warning: net/rxrpc/rxgk_app.c:65 rxgk_yfs_decode_ticket() warn: untrusted unsigned subtract. 'ticket_len - 10 * 4' by prechecking the length of what we're trying to extract in two places in the token and decoding for a response packet. Also use sizeof() on the struct we're extracting rather specifying the size numerically to be consistent with the other related statements.	N/A	More Details
CVE-2025-39961	In the Linux kernel, the following vulnerability has been resolved: iommu/amd/pgtbl: Fix possible race while increase page table level The AMD IOMMU host page table implementation supports dynamic page table levels (up to 6 levels), starting with a 3-level configuration that expands based on IOVA address. The kernel maintains a root pointer and current page table level to enable proper page table walks in alloc_pte()/fetch_pte() operations. The IOMMU IOVA allocator initially starts with 32-bit address and onces its exhuasted it switches to 64-bit address (max address is determined based on IOMMU and device DMA capability). To support larger IOVA, AMD IOMMU driver increases page table level. But in unmap path (iommu_v1_unmap_pages()), fetch_pte() reads pgtable->[root/mode] without lock. So its possible that in exteme corner case, when increase_address_space() is updating pgtable->[root/mode], fetch_pte() reads wrong page table level (pgtable->mode). It does compare the value with level encoded in page table and returns NULL. This will result is iommu_unmap ops to fail and upper layer may retry/log WARN_ON. CPU 0 CPU 1 ------ ------ map pages unmap pages alloc_pte() -> increase_address_space() iommu_v1_unmap_pages() -> fetch_pte() pgtable->root = pte (new root value) READ pgtable->[mode/root] Reads new root, old mode Updates mode (pgtable->mode += 1) Since Page table level updates are infrequent and already synchronized with a spinlock, implement seqcount to enable lock-free read operations on the read path.	N/A	More Details
CVE-2025-39960	In the Linux kernel, the following vulnerability has been resolved: gpiolib: acpi: initialize acpi_gpio_info struct Since commit 7c010d463372 ("gpiolib: acpi: Make sure we fill struct acpi_gpio_info"), uninitialized acpi_gpio_info struct are passed to __acpi_find_gpio() and later in the call stack info->quirks is used in acpi_populate_gpio_lookup. This breaks the i2c_hid_cpi driver: [58.122916] i2c_hid_acpi i2c-UNIW0001:00: HID over i2c has not been provided an Int	N/A	More Details

	IRQ [58.123097] i2c_hid_acpi i2c-UNIW0001:00: probe with driver i2c_hid_acpi failed with error -22 Fix this by initializing the acpi_gpio_info pass to __acpi_find_gpio()		
CVE-2025-39959	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: Fix incorrect retrival of acp_chip_info Use dev_get_drvdata(dev->parent) instead of dev_get_platdata(dev) to correctly obtain acp_chip_info members in the acp I2S driver. Previously, some members were not updated properly due to incorrect data access, which could potentially lead to null pointer dereferences. This issue was missed in the earlier commit ("ASoC: amd: acp: Fix NULL pointer deref in acp_i2s_set_tdm_slot"), which only addressed set_tdm_slot(). This change ensures that all relevant functions correctly retrieve acp_chip_info, preventing further null pointer dereference issues.	N/A	More Details
CVE-2025-39958	In the Linux kernel, the following vulnerability has been resolved: iommu/s390: Make attach succeed when the device was surprise removed When a PCI device is removed with surprise hotplug, there may still be attempts to attach the device to the default domain as part of tear down via (__iommu_release_dma_ownership()), or because the removal happens during probe (__iommu_probe_device()). In both cases zpci_register_ioat() fails with a cc value indicating that the device handle is invalid. This is because the device is no longer part of the instance as far as the hypervisor is concerned. Currently this leads to an error return and s390_iommu_attach_device() fails. This triggers the WARN_ON() in __iommu_group_set_domain_nofail() because attaching to the default domain must never fail. With the device fenced by the hypervisor no DMAs to or from memory are possible and the IOMMU translations have no effect. Proceed as if the registration was successful and let the hotplug event handling clean up the device. This is similar to how devices in the error state are handled since commit 59bbf596791b ("iommu/s390: Make attach succeed even if the device is in error state") except that for removal the domain will not be registered later. This approach was also previously discussed at the link. Handle both cases, error state and removal, in a helper which checks if the error needs to be propagated or ignored. Avoid magic number condition codes by using the pre-existing, but never used, defines for PCI load/store condition codes and rename them to reflect that they apply to all PCI instructions.	N/A	More Details
CVE-2025-39957	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: increase scan_ies_len for S1G Currently the S1G capability element is not taken into account for the scan_ies_len, which leads to a buffer length validation failure in ieee80211_prep_hw_scan() and subsequent WARN in __ieee80211_start_scan(). This prevents hw scanning from functioning. To fix ensure we accommodate for the S1G capability length.	N/A	More Details
CVE-2025-39956	In the Linux kernel, the following vulnerability has been resolved: igc: don't fail igc_probe() on LED setup error When igc_led_setup() fails, igc_probe() fails and triggers kernel panic in free_netdev() since unregister_netdev() is not called. [1] This behavior can be tested using fault-injection framework, especially the failslab feature. [2] Since LED support is not mandatory, treat LED setup failures as non-fatal and continue probe with a warning message, consequently avoiding the kernel panic. [1] kernel BUG at net/core/dev.c:12047! Oops: invalid opcode: 0000 [#1] SMP NOPTI CPU: 0 UID: 0 PID: 937 Comm: repro-igc-led-e Not tainted 6.17.0-rc4-enjuk-tnguy-00865-gc4940196ab02 #64 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:free_netdev+0x278/0x2b0 [...] Call Trace: <TASK> igc_probe+0x370/0x910 local_pci_probe+0x3a/0x80 pci_device_probe+0xd1/0x200 [...] [2] #!/bin/bash -ex FAILSLAB_PATH=/sys/kernel/debug/failslab/ DEVICE=0000:00:05.0 START_ADDR=$(grep " igc_led_setup" /proc/kallsyms | awk '{printf("0x%s", $1)}') END_ADDR=$(printf "0x%x" $((START_ADDR + 0x100))) echo $START_ADDR > $FAILSLAB_PATH/require-start echo $END_ADDR > $FAILSLAB_PATH/require-end echo 1 > $FAILSLAB_PATH/times echo 100 > $FAILSLAB_PATH/probability echo N > $FAILSLAB_PATH/ignore-gfp-wait echo $DEVICE > /sys/bus/pci/drivers/igc/bind	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: tcp: Clear tcp_sk(sk)->fastopen_rsk in tcp_disconnect(). syzbot reported the splat below where a socket had tcp_sk(sk)->fastopen_rsk in the TCP_ESTABLISHED state. [0] syzbot reused the server-side TCP Fast Open socket as a new client before the TFO socket completes 3WHS: 1. accept() 2. connect(AF_UNSPEC) 3. connect() to another destination As of accept(), sk->sk_state is TCP_SYN_RECV, and tcp_disconnect() changes it to TCP_CLOSE and makes connect() possible, which restarts timers. Since tcp_disconnect() forgot to clear tcp_sk(sk)->fastopen_rsk, the retransmit timer triggered the warning and the intended packet was not retransmitted. Let's		

CVE-2025-39955	call reqsk_fastopen_remove() in tcp_disconnect(). [0]: WARNING: CPU: 2 PID: 0 at net/ipv4/tcp_timer.c:542 tcp_retransmit_timer (net/ipv4/tcp_timer.c:542 (discriminator 7)) Modules linked in: CPU: 2 UID: 0 PID: 0 Comm: swapper/2 Not tainted 6.17.0-rc5-g201825fb4278 #62 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:tcp_retransmit_timer (net/ipv4/tcp_timer.c:542 (discriminator 7)) Code: 41 55 41 54 55 53 48 8b af b8 08 00 00 48 89 fb 48 85 ed 0f 84 55 01 00 00 0f b6 47 12 3c 03 74 0c 0f b6 47 12 3c 04 74 04 90 <0f> 0b 90 48 8b 85 c0 00 00 00 48 89 ef 48 8b 40 30 e8 6a 4f 06 3e RSP: 0018:ffffc900002f8d40 EFLAGS: 00010293 RAX: 0000000000000002 RBX: ffff888106911400 RCX: 0000000000000017 RDX: 0000000002517619 RSI: ffffffff83764080 RDI: ffff888106911400 RBP: ffff888106d5c000 R08: 0000000000000001 R09: ffffc900002f8de8 R10: 00000000000000c2 R11: ffffc900002f8ff8 R12: ffff888106911540 R13: ffff888106911480 R14: ffff888106911840 R15: ffffc900002f8de0 FS: 0000000000000000(0000) GS:ffff88907b768000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f8044d69d90 CR3: 0000000002c30003 CR4: 0000000000370ef0 Call Trace: <IRQ> tcp_write_timer (net/ipv4/tcp_timer.c:738) call_timer_fn (kernel/time/timer.c:1747) __run_timers (kernel/time/timer.c:1799 kernel/time/timer.c:2372) timer_expire_remote (kernel/time/timer.c:2385 kernel/time/timer.c:2376 kernel/time/timer.c:2135) tmigr_handle_remote_up (kernel/time/timer_migration.c:944 kernel/time/timer_migration.c:1035) __walk_groups.isra.0 (kernel/time/timer_migration.c:533 (discriminator 1)) tmigr_handle_remote (kernel/time/timer_migration.c:1096) handle_softirqs (./arch/x86/include/asm/jump_label.h:36 ./include/trace/events/irq.h:142 kernel/softirq.c:580) irq_exit_rcu (kernel/softirq.c:614 kernel/softirq.c:453 kernel/softirq.c:680 kernel/softirq.c:696) sysvec_apic_timer_interrupt (arch/x86/kernel/apic/apic.c:1050 (discriminator 35) arch/x86/kernel/apic/apic.c:1050 (discriminator 35)) </IRQ>	N/A	More Details
CVE-2025-39954	In the Linux kernel, the following vulnerability has been resolved: clk: sunxi-ng: mp: Fix dual-divider clock rate readback When dual-divider clock support was introduced, the P divider offset was left out of the .recalc_rate readback function. This causes the clock rate to become bogus or even zero (possibly due to the P divider being 1, leading to a divide-by-zero). Fix this by incorporating the P divider offset into the calculation.	N/A	More Details
CVE-2025-11535	MongoDB Connector for BI installation via MSI on Windows leaves ACLs unset on custom install directories allows Privilege Escalation.This issue affects MongoDB Connector for BI: from 2.0.0 through 2.14.24.	N/A	More Details
CVE-2017-20202	Web Developer for Chrome v0.4.9 contained malicious code that generated a domain via a DGA and fetched a remote script. The fetched script conditionally loaded follow-on modules that performed extensive ad substitution and malvertising, displayed fake “repair” alerts that redirected users to affiliate programs, and attempted to harvest credentials when users logged in. Injected components enumerate common banner sizes for substitution, replace third-party ad calls, and redirect victim traffic to affiliate landing pages. Potential impacts include user-level code execution in the browser context, large-scale ad fraud and traffic hijacking, credential theft, and exposure to additional payloads delivered by the actor. The compromise was reported on by the maintainer of Web Developer for Chrome on August 2, 2017 and remediated in v0.5.0.	N/A	More Details
CVE-2017-20201	CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 (32-bit builds) contained a malicious pre-entry-point loader that diverts execution from __scrt_common_main_seh into a custom loader. That loader decodes an embedded blob into shellcode, allocates executable heap memory, resolves Windows API functions at runtime, and transfers execution to an in-memory payload. The payload performs anti-analysis checks, gathers host telemetry, encodes the data with a two-stage obfuscation, and attempts HTTPS exfiltration to hard-coded C2 servers or month-based DGA domains. Potential impacts include remote data collection and exfiltration, stealthy in-memory execution and persistence, and potential lateral movement. CCleaner was developed by Piriform, which was acquired by Avast in July 2017; Avast later merged with NortonLifeLock to form the parent company now known as Gen Digital. According to vendor advisories, the compromised CCleaner build was released on August 15, 2017 and remediated on September 12, 2017 with v5.34; the compromised CCleaner Cloud build was released on August 24, 2017 and remediated on September 15, 2017 with v1.07.3214.	N/A	More Details
CVE-	An improper input neutralization vulnerability in the management web interface of the Palo Alto Networks PAN-OS® software enables an authenticated administrator to bypass system		

2025-4615	restrictions and execute arbitrary commands. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators. Cloud NGFW and Prisma® Access are not affected by this vulnerability.	N/A	More Details
CVE-2025-34267	Flowise v3.0.1 < 3.0.8 and all versions after with 'ALLOW_BUILTIN_DEP' enabled contain an authenticated remote code execution vulnerability and node VM sandbox escape due to insecure use of integrated modules (Puppeteer and Playwright) within the nodevm execution environment. An authenticated attacker able to create or run a tool that leverages Puppeteer/Playwright can specify attacker-controlled browser binary paths and parameters. When the tool executes, the attacker-controlled executable/parameters are run on the host and circumvent the intended nodevm sandbox restrictions, resulting in execution of arbitrary code in the context of the host. This vulnerability was incorrectly assigned as a duplicate CVE-2025-26319 by the developers and should be considered distinct from that identifier.	N/A	More Details
CVE-2025-5009	In Gemini iOS, when a user shared a snippet of a conversation, it would share the entire conversation via a sharable public link that contained the entire conversation history and not just the snippet.	N/A	More Details
CVE-2025-61672	Synapse is an open source Matrix homeserver implementation. Lack of validation for device keys in Synapse before 1.138.3 and in Synapse 1.139.0 allow an attacker registered on the victim homeserver to degrade federation functionality, unpredictably breaking outbound federation to other homeservers. The issue is patched in Synapse 1.138.3, 1.138.4, 1.139.1, and 1.139.2. Note that even though 1.138.3 and 1.139.1 fix the vulnerability, they inadvertently introduced an unrelated regression. For this reason, the maintainers of Synapse recommend skipping these releases and upgrading straight to 1.138.4 and 1.139.2.	N/A	More Details
CVE-2025-40640	Stored Cross-Site Scripting (XSS) vulnerability in Energy CRM v2025 by Status Tracker Ltd, consisting of a stored XSS due to lack of proper validation of user input by sending a POST request to “/crm/create_invoice_submit.php”, using the “customerName_0” parameter. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	N/A	More Details
CVE-2025-9554	Vulnerability in Drupal Owl Carousel 2.This issue affects Owl Carousel 2: *.*.	N/A	More Details
CVE-2025-41088	Stored Cross-Site Scripting (XSS) in Xibo Signage's Xibo CMS v4.1.2, due to a lack of proper validation of user input. To exploit the vulnerability, the attacker must create a template in the 'Templates' section, then add a text element in the 'Global Elements' section, and finally modify the 'Text' field in the section with the malicious payload.	N/A	More Details
CVE-2025-7328	Multiple Broken Authentication security issues exist in the affected product. The security issues are due to missing authentication checks on critical functions. These could result in potential denial-of-service, admin account takeover, or NAT rule modifications. Devices would no longer be able to communicate through NATR as a result of denial-of-service or NAT rule modifications. NAT rule modification could also result in device communication to incorrect endpoints. Admin account takeover could allow modification of configuration and require physical access to restore.	N/A	More Details
CVE-2025-11720	The Firefox and Firefox Focus UI for the Android custom tab feature only showed the "site" that was loaded, not the full hostname. User supplied content hosted on a subdomain of a site could have been used to fool a user into thinking it was content from a different subdomain of that site. This vulnerability affects Firefox < 144.	N/A	More Details
CVE-2025-11719	Starting in Firefox 143, the use of the native messaging API by web extensions on Windows could lead to crashes caused by use-after-free memory corruption. This vulnerability affects Firefox < 144 and Thunderbird < 144.	N/A	More Details
CVE-2025-11718	When the address bar was hidden due to scrolling on Android, a malicious page could create a fake address bar to fool the user in response to a visibilitychange event This vulnerability affects Firefox < 144.	N/A	More Details
CVE-2025-11717	When switching between Android apps using the card carousel Firefox shows a black screen as its card image when a password-related screen was the last one being used. Prior to Firefox 144 the password edit screen was visible. This vulnerability affects Firefox < 144.	N/A	More Details

CVE-2025-11716	Links in a sandboxed iframe could open an external app on Android without the required "allow-" permission. This vulnerability affects Firefox < 144 and Thunderbird < 144.	N/A	More Details
CVE-2025-11715	Memory safety bugs present in Firefox ESR 140.3, Thunderbird ESR 140.3, Firefox 143 and Thunderbird 143. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11714	Memory safety bugs present in Firefox ESR 115.28, Firefox ESR 140.3, Thunderbird ESR 140.3, Firefox 143 and Thunderbird 143. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11713	Insufficient escaping in the “Copy as cURL” feature could have been used to trick a user into executing unexpected code on Windows. This did not affect Firefox running on other operating systems. This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11712	A malicious page could have used the type attribute of an OBJECT tag to override the default browser behavior when encountering a web resource served without a content-type. This could have contributed to an XSS on a site that unsafely serves files without a content-type header. This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11711	There was a way to change the value of JavaScript Object properties that were supposed to be non-writeable. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11710	A compromised web process using malicious IPC messages could have caused the privileged browser process to reveal blocks of its memory to the compromised process. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11709	A compromised web process was able to trigger out of bounds reads and writes in a more privileged process using manipulated WebGL textures. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-11708	Use-after-free in MediaTrackGraphImpl::GetInstance() This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	N/A	More Details
CVE-2025-9437	A security issue exists within the Studio 5000 Logix Designer add-on profile (AOP) for the ArmorStart Classic distributed motor controller, resulting in denial-of-service. This vulnerability is possible due to the input of invalid values into Component Object Model (COM) methods.	N/A	More Details
CVE-2025-55078	In Eclipse ThreadX before version 6.4.3, an attacker can cause a denial of service (crash) by providing a pointer to a reserved or unmapped memory region. Vulnerable system calls had a check of pointers, but that check wasn't verifying whether the pointer is outside the module memory region.	N/A	More Details
CVE-2025-62365	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. Prior to 25.7.0, there is a reflected-XSS in `report_this` function in `librenms/includes/functions.php`. The `report_this` function had improper filtering (`htmlentities` function was incorrectly use in a href environment), which caused the `project_issues` parameter to trigger an XSS vulnerability. This vulnerability is fixed in 25.7.0.	N/A	More Details
CVE-2025-62362	gpp-burgerportaal is a Dutch government citizen portal application. In versions before 2.0.3, 3.0.2, and 4.0.1, the name and email address of employees who publish content are exposed in network responses and can be discovered by viewing the browser's developer tools network tab. This information disclosure may violate employee privacy expectations and could be used for targeted attacks or unwanted contact. This issue has been patched in versions 2.0.3, 3.0.2,	N/A	More Details

	and 4.0.1. No known workarounds exist.		
CVE-2025-62361	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.0, an Open Redirect vulnerability was identified in the control.php endpoint of the WeGIA application, specifically in the nextPage parameter (metodo=listarTodos nomeClasse=AlmoxarifeControle). This vulnerability allows attackers to redirect users to arbitrary external domains, enabling phishing campaigns, malicious payload distribution, or user credential theft. This vulnerability is fixed in 3.5.0.	N/A	More Details
CVE-2025-62360	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users.Prior to 3.5.1, a SQL Injection vulnerability was identified in the /html/funcionario/dependente_documento.php endpoint, specifically in the id_dependente parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This vulnerability is fixed in 3.5.1.	N/A	More Details
CVE-2025-11721	Memory safety bug present in Firefox 143 and Thunderbird 143. This bug showed evidence of memory corruption and we presume that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144 and Thunderbird < 144.	N/A	More Details
CVE-2025-7329	A Stored Cross-Site Scripting security issue exists in the affected product that could potentially allow a malicious user to view and modify sensitive data or make the webpage unavailable. The vulnerability stems from missing special character filtering and encoding. Successful exploitation requires an attacker to be able to update configuration fields behind admin login.	N/A	More Details
CVE-2025-62251	Liferay Portal 7.3.0 through 7.4.3.119, and Liferay DXP 2023.Q3.1 through 2023.Q3.8, 2023.Q4.0 through 2023.Q4.5, 7.4 GA through update 92 and 7.3 GA though update 36 shows content to users who do not have permission to view it via the Menu Display Widget. This security flaw could result in sensitive information being exposed to unauthorized users.	N/A	More Details
CVE-2025-7330	A cross-site request forgery security issue exists in the product and version listed. The vulnerability stems from missing CSRF checks on the impacted form. This allows for unintended configuration modification if an attacker can convince a logged in admin to visit a crafted link.	N/A	More Details
CVE-2025-25255	An Improperly Implemented Security Check for Standard vulnerability [CWE-358] in FortiProxy 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0.1 through 7.0.21, and FortiOS 7.6.0 through 7.6.3 explicit web proxy may allow an authenticated proxy user to bypass the domain fronting protection feature via crafted HTTP requests.	N/A	More Details
CVE-2025-11577	Clevo’s UEFI firmware update packages, including B10717.exe, inadvertently contained private signing keys used for Boot Guard and Boot Policy Manifest verification. The exposure of these keys could allow attackers to sign malicious firmware that appears trusted by affected systems, undermining the integrity of the early boot process.	N/A	More Details
CVE-2025-62157	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Argo Workflows versions prior to 3.6.12 and versions 3.7.0 through 3.7.2 expose artifact repository credentials in plaintext in workflow-controller pod logs. An attacker with permissions to read pod logs in a namespace running Argo Workflows can read the workflow-controller logs and obtain credentials to the artifact repository. Update to versions 3.6.12 or 3.7.3 to remediate the vulnerability. No known workarounds exist.	N/A	More Details
CVE-2025-62172	Home Assistant is open source home automation software that puts local control and privacy first. In versions 2025.1.0 through 2025.10.1, the energy dashboard is vulnerable to stored cross-site scripting. An authenticated user can inject malicious JavaScript code into an energy entity's name field, which is then executed when any user hovers over data points in the energy dashboard graph tooltips. The vulnerability exists because entity names containing HTML are not properly sanitized before being rendered in graph tooltips. This could allow an attacker with authentication to execute arbitrary JavaScript in the context of other users' sessions. Additionally, if an energy provider (such as Tibber) supplies a malicious default name for an entity, the vulnerability can be exploited without direct user action when the default name is used. This issue has been patched in version 2025.10.2. No known workarounds exist.	N/A	More Details
	mailgen is a Node.js package that generates responsive HTML e-mails for sending		

CVE-2025-62366	transactional mail. Mailgen versions through 2.0.30 contain an HTML injection vulnerability in plaintext emails produced by the generatePlaintext method when user-generated content is supplied. The function attempts to remove HTML tags, but if tags are provided as encoded HTML entities they are not removed and are later decoded, resulting in active HTML (for example an img tag with an event handler) in the supposed plaintext output. In contexts where the generated plaintext string is subsequently rendered as HTML, this can allow execution of attacker-controlled JavaScript. Versions 2.0.31 and later contain a fix. No known workarounds exist.	N/A	More Details
CVE-2025-33044	APTIOV contains a vulnerability in BIOS where an attacker may cause an Improper Restriction of Operations within the Bounds of a Memory Buffer by local means. Successful exploitation of this vulnerability may lead to memory corruption and impact Integrity and Availability.	N/A	More Details
CVE-2025-11548	A remote, unauthenticated privilege escalation in ibi WebFOCUS allows an attacker to gain administrative access to the application which may lead to unauthenticated Remote Code Execution	N/A	More Details
CVE-2025-22833	APTIOV contains a vulnerability in BIOS where an attacker may cause a Buffer Copy without Checking Size of Input by local accessing. Successful exploitation of this vulnerability may lead to arbitrary code execution.	N/A	More Details
CVE-2025-22832	APTIOV contains a vulnerability in BIOS where an attacker may cause an Out-of-bounds Write by local. Successful exploitation of this vulnerability may lead to data corruption and loss of availability.	N/A	More Details
CVE-2025-22831	APTIOV contains a vulnerability in BIOS where an attacker may cause an Out-of-bounds Write by local. Successful exploitation of this vulnerability may lead to data corruption and loss of availability.	N/A	More Details
CVE-2025-36730	A prompt injection vulnerability exists in Windsurft version 1.10.7 in Write mode using SWE-1 model. It is possible to create a file name that will be appended to the user prompt causing Windsurf to follow its instructions.	N/A	More Details
CVE-2025-9178	A denial-of-service security issue exists in the affected product and version. The security issue is caused through CIP communication using crafted payloads. The security issue could result in no CIP communication with 1715 EtherNet/IP Adapter.A restart is required to recover.	N/A	More Details
CVE-2025-9177	A denial-of-service security issue exists in the affected product and version. The security issue stems from a high number of requests sent to the web server. This could result in a web server crash however; this does not impact I/O control or communication . A power cycle is required to recover and utilize the webpage.	N/A	More Details
CVE-2025-9124	A denial-of-service security issue in the affected product. The security issue stems from a fault occurring when a crafted CIP unconnected explicit message is sent. This can result in a major non-recoverable fault.	N/A	More Details
CVE-2025-9068	A security issue exists within the Rockwell Automation Driver Package x64 Microsoft Installer File (MSI) repair functionality, installed with FTLinx. Authenticated attackers with valid Windows Users credentials can initiate a repair and hijack the resulting console window for vbpinstall.exe. This allows the launching of a command prompt running with SYSTEM-level privileges, allowing full access to all files, processes, and system resources.	N/A	More Details
CVE-2025-9067	A security issue exists within the x86 Microsoft Installer File (MSI), installed with FTLinx. Authenticated attackers with valid Windows user credentials can initiate a repair and hijack the resulting console window. This allows the launching of a command prompt running with SYSTEM-level privileges, allowing full access to all files, processes, and system resources.	N/A	More Details
CVE-2025-9066	A security issue was discovered within FactoryTalk® ViewPoint, allowing unauthenticated attackers to achieve XXE. Certain SOAP requests can be abused to perform XXE, resulting in a temporary denial-of-service.	N/A	More Details
CVE-2025-9064	A path traversal security issue exists within FactoryTalk View Machine Edition, allowing unauthenticated attackers on the same network as the device to delete any file within the panels operating system. Exploitation of this vulnerability is dependent on the knowledge of filenames to be deleted.	N/A	More Details

CVE-2025-9063	An authentication bypass security issue exists within FactoryTalk View Machine Edition Web Browser ActiveX control. Exploitation of this vulnerability allows unauthorized access to the PanelView Plus 7 Series B, including access to the file system, retrieval of diagnostic information, event logs, and more.	N/A	More Details
CVE-2025-62359	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.0, a Reflected Cross-Site Scripting (XSS) vulnerability was identified in the /pet/profile_pet.php?id_pet= endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the id_pet parameter. This vulnerability is fixed in 3.5.0.	N/A	More Details
CVE-2025-62179	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.1, a SQL Injection vulnerability was identified in the /html/funcionario/cadastro_funcionario_pessoa_existente.php endpoint, specifically in the cpf parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This vulnerability is fixed in 3.5.1.	N/A	More Details
CVE-2025-41089	Reflected Cross-Site Scripting (XSS) in Xibo CMS v4.1.2 from Xibo Signage, due to a lack of proper validation of user input. To exploit the vulnerability, the attacker must create a template in the 'Templates' section, then add an element that has the 'Configuration Name' field, such as the 'Clock' widget. Next, modify the 'Configuration Name' field in the left-hand section.	N/A	More Details
CVE-2025-9553	Vulnerability in Drupal API Key manager.This issue affects API Key manager: *.*.	N/A	More Details
CVE-2025-9551	Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Protected Pages allows Brute Force.This issue affects Protected Pages: from 0.0.0 before 1.8.0.	N/A	More Details
CVE-2025-9550	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Facets allows Cross-Site Scripting (XSS).This issue affects Facets: from 0.0.0 before 2.0.10, from 3.0.0 before 3.0.1.	N/A	More Details
CVE-2025-9549	Missing Authorization vulnerability in Drupal Facets allows Forceful Browsing.This issue affects Facets: from 0.0.0 before 2.0.10, from 3.0.0 before 3.0.1.	N/A	More Details
CVE-2025-8093	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Authenticator Login allows Authentication Bypass.This issue affects Authenticator Login: from 0.0.0 before 2.1.8.	N/A	More Details
CVE-2025-62159	External Secrets Operator reads information from a third-party service and automatically injects the values as Kubernetes Secrets. A vulnerability was discovered in the BeyondTrust provider implementation for External Secrets Operator versions 0.10.1 through 0.19.2. The provider previously retrieved Kubernetes secrets directly, without validating the namespace context or the type of secret store. This allowed unauthorized cross-namespace secret access, violating security boundaries and potentially exposing sensitive credentials. In version 0.20.0, the provider code was updated to use the `resolvers.SecretKeyRef` utility, which enforces namespace validation and only allows cross-namespace access for `ClusterSecretStore` types. This ensures secrets are only retrieved from the correct namespace, mitigating the risk of unauthorized access. All users should upgrade to the latest version containing this fix. As a workaround, use a policy engine such as Kyverno or OPA to prevent using BeyondTrust provider and/or validate the `(Cluster)SecretStore` and ensure the namespace may only be set when using a `ClusterSecretStore`.	N/A	More Details
CVE-2025-52885	Poppler ia a library for rendering PDF files, and examining or modifying their structure. A use-after-free (write) vulnerability has been detected in versions Poppler prior to 25.10.0 within the StructTreeRoot class. The issue arises from the use of raw pointers to elements of a `std::vector`, which can lead to dangling pointers when the vector is resized. The vulnerability stems from the way that refToParentMap stores references to `std::vector` elements using raw pointers. These pointers may become invalid when the vector is resized. This vulnerability is a common security problem involving the use of raw pointers to `std::vectors`. Internally,	N/A	More Details

	`std::vector `stores its elements in a dynamically allocated array. When the array reaches its capacity and a new element is added, the vector reallocates a larger block of memory and moves all the existing elements to the new location. At this point if any pointers to elements are stored before a resize occurs, they become dangling pointers once the reallocation happens. Version 25.10.0 contains a patch for the issue.		
CVE-2025-61912	python-ldap is a lightweight directory access protocol (LDAP) client API for Python. In versions prior to 3.4.5, ldap.dn.escape_dn_chars() escapes \x00 incorrectly by emitting a backslash followed by a literal NUL byte instead of the RFC-4514 hex form \00. Any application that uses this helper to construct DNs from untrusted input can be made to consistently fail before a request is sent to the LDAP server (e.g., AD), resulting in a client-side denial of service. Version 3.4.5 contains a patch for the issue.	N/A	More Details
CVE-2025-61911	python-ldap is a lightweight directory access protocol (LDAP) client API for Python. In versions prior to 3.4.5, the sanitization method `ldap.filter.escape_filter_chars` can be tricked to skip escaping of special characters when a crafted `list` or `dict` is supplied as the `assertion_value` parameter, and the non-default `escape_mode=1` is configured. The method `ldap.filter.escape_filter_chars` supports 3 different escaping modes. `escape_mode=0` (default) and `escape_mode=2` happen to raise exceptions when a `list` or `dict` object is supplied as the `assertion_value` parameter. However, `escape_mode=1` computes without performing adequate logic to ensure a fully escaped return value. If an application relies on the vulnerable method in the `python-ldap` library to escape untrusted user input, an attacker might be able to abuse the vulnerability to launch ldap injection attacks which could potentially disclose or manipulate ldap data meant to be inaccessible to them. Version 3.4.5 fixes the issue by adding a type check at the start of the `ldap.filter.escape_filter_chars` method to raise an exception when the supplied `assertion_value` parameter is not of type `str`.	N/A	More Details
CVE-2025-62245	Cross-site request forgery (CSRF) vulnerability in Liferay Portal 7.4.1 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.10, and 7.4 GA through update 92 allows remote attackers to add and edit publication comments.	N/A	More Details
CVE-2025-62158	Frappe Learning is a learning system that helps users structure their content. In versions prior to 2.38.0, the system did stored the attachments uploaded by the students in their assignments as public files. This issue potentially exposed student-uploaded files to the public. Anyone with the file URL could access these files without authentication. The issue has been fixed in version 2.38.0 by ensuring all student-uploaded assignment attachments are stored as private files by default.	N/A	More Details
CVE-2025-61927	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. Happy DOM v19 and lower contains a security vulnerability that puts the owner system at the risk of RCE (Remote Code Execution) attacks. A Node.js VM Context is not an isolated environment, and if the user runs untrusted JavaScript code within the Happy DOM VM Context, it may escape the VM and get access to process level functionality. It seems like what the attacker can get control over depends on if the process is using ESM or CommonJS. With CommonJS the attacker can get hold of the `require()` function to import modules. Happy DOM has JavaScript evaluation enabled by default. This may not be obvious to the consumer of Happy DOM and can potentially put the user at risk if untrusted code is executed within the environment. Version 20.0.0 patches the issue by changing JavaScript evaluation to be disabled by default.	N/A	More Details
CVE-2025-61921	Sinatra is a domain-specific language for creating web applications in Ruby. In versions prior to 4.2.0, there is a denial of service vulnerability in the `If-Match` and `If-None-Match` header parsing component of Sinatra, if the `etag` method is used when constructing the response. Carefully crafted input can cause `If-Match` and `If-None-Match` header parsing in Sinatra to take an unexpected amount of time, possibly resulting in a denial of service attack vector. This header is typically involved in generating the `ETag` header value. Any applications that use the `etag` method when generating a response are impacted. Version 4.2.0 fixes the issue.	N/A	More Details
CVE-2025-61689	HTTP.jl is an HTTP client and server functionality for the Julia programming language. Prior to version 1.10.19, HTTP.jl did not validate header names/values for illegal characters, allowing CRLF-based header injection and response splitting. This enables HTTP response splitting and header injection, leading to cache poisoning, XSS, session fixation, and more. This issue is	N/A	More Details

	fixed in HTTP.jl `v1.10.19`.		
CVE-2025-60307	code-projects Computer Laboratory System 1.0 has a SQL injection vulnerability, where entering a universal password in the Password field on the login page can bypass login attempts.	N/A	More Details
CVE-2025-60305	SourceCodester Online Student Clearance System 1.0 is vulnerable to Incorrect Access Control. The application contains a logic flaw which allows low privilege users can forge high privileged sessions and perform sensitive operations.	N/A	More Details
CVE-2025-48043	Incorrect Authorization vulnerability in ash-project ash allows Authentication Bypass. This vulnerability is associated with program files lib/ash/policy/authorizer/authorizer.ex and program routines 'Elixir.Ash.Policy.Authorizer':strict_filters/2. This issue affects ash: from pkg:hex/ash@0 before pkg:hex/ash@3.6.2, before 3.6.2, before 66d81300065b970da0d2f4528354835d2418c7ae.	N/A	More Details
CVE-2025-62239	Cross-site scripting (XSS) vulnerability in workflow process builder in Liferay Portal 7.4.3.21 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 21 through update 92 allows remote authenticated attackers to inject arbitrary web script or HTML via the crafted input in a workflow definition.	N/A	More Details
CVE-2025-62238	Stored cross-site scripting (XSS) vulnerability on the Membership page in Account Settings in Liferay Portal 7.4.3.21 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 21 through update 92 allows remote authenticated attackers to inject arbitrary web script or HTML via a crafted payload injected into a Account's “Name“ text field.	N/A	More Details
CVE-2025-62237	Stored cross-site scripting (XSS) vulnerability in Commerce’s view order page in Liferay Portal 7.4.3.8 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 8 through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an Account’s “Name” text field.	N/A	More Details
CVE-2025-9552	Vulnerability in Drupal Synchronize composer.Json With Contrib Modules.This issue affects Synchronize composer.Json With Contrib Modules: *.*.	N/A	More Details
CVE-2025-27258	Ericsson Network Manager (ENM) versions prior to ENM 25.1 GA contain a vulnerability, if exploited, can result in an escalation of privilege.	N/A	More Details
CVE-2025-62177	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Prior to 3.5.1, a SQL Injection vulnerability was identified in the /html/funcionario/dependente_listar.php endpoint, specifically in the id_funcionario parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This vulnerability is fixed in 3.5.1.	N/A	More Details
CVE-2025-27259	Ericsson Network Manager versions prior to ENM 25.2 GA contain a vulnerability that, if exploited, can exfiltrate limited data or redirect victims to other sites or domains.	N/A	More Details
CVE-2025-62252	Insecure Direct Object Reference (IDOR) vulnerability in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows remote authenticated users in one virtual instance to assign an organization to a user in a different virtual instance via the _com_liferay_users_admin_web_portlet_UsersAdminPortlet_addUserIds parameter.	N/A	More Details
CVE-2025-62246	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, and older unsupported versions allow remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a user’s first, middle or last name text field to (1) page comments widget, (2) blog entry comments, (3) document and media document comments, (4) message board messages, (5) wiki page comments or (6) other widgets/apps that supports mentions.	N/A	More Details

CVE-2024-6211	Rejected reason: loading template...	N/A	More Details
CVE-2025-62242	Insecure Direct Object Reference (IDOR) vulnerability with account addresses in Liferay Portal 7.4.3.4 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote authenticated users to from one account to view addresses from a different account via the _com_liferay_account_admin_web_internal_portlet_AccountEntriesAdminPortlet_addressId parameter.	N/A	More Details
CVE-2025-62241	Insecure Direct Object Reference (IDOR) vulnerability with shipment addresses in Liferay DXP 2023.Q4.1 through 2023.Q4.5 allows remote authenticated users to from one virtual instance to view the shipment addresses of different virtual instance via the _com_liferay_commerce_order_web_internal_portlet_CommerceOrderPortlet_commerceOrderId parameter.	N/A	More Details
CVE-2025-62243	Insecure direct object reference (IDOR) vulnerability in Publications in Liferay Portal 7.4.1 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote authenticated attackers to view publication comments via the _com_liferay_change_tracking_web_portlet_PublicationsPortlet_value parameter. Publications comments in Liferay Portal 7.4.1 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 does not properly check user permissions, which allows remote authenticated users to edit publication comments via crafted URLs.	N/A	More Details
CVE-2025-61775	Vickey is a Misskey-based microblogging platform. A vulnerability exists in Vickey prior to version 2025.10.0 where unexpired email confirmation links can be reused multiple times to send repeated confirmation emails to a verified email address. Under certain conditions, a verified email address could receive repeated confirmation messages if the verification link was accessed multiple times. This issue may result in unintended email traffic but does not expose user data. The issue was addressed in version 2025.10.0 by improving validation logic to ensure verification links behave as expected after completion.	N/A	More Details
CVE-2025-7707	The llama_index library version 0.12.33 sets the NLTK data directory to a subdirectory of the codebase by default, which is world-writable in multi-user environments. This configuration allows local users to overwrite, delete, or corrupt NLTK data files, leading to potential denial of service, data tampering, or privilege escalation. The vulnerability arises from the use of a shared cache directory instead of a user-specific one, making it susceptible to local data tampering and denial of service.	N/A	More Details
CVE-2025-62244	Insecure direct object reference (IDOR) vulnerability in Publications in Liferay Portal 7.3.1 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92, and 7.3 GA through update 36 allows remote authenticated attackers to view the edit page of a publication via the _com_liferay_change_tracking_web_portlet_PublicationsPortlet_ctCollectionId parameter.	N/A	More Details
CVE-2025-39965	In the Linux kernel, the following vulnerability has been resolved: xfrm: xfrm_alloc_spi shouldn't use 0 as SPI x->id.spi == 0 means "no SPI assigned", but since commit 94f39804d891 ("xfrm: Duplicate SPI Handling"), we now create states and add them to the byspi list with this value. __xfrm_state_delete doesn't remove those states from the byspi list, since they shouldn't be there, and this shows up as a UAF the next time we go through the byspi list.	N/A	More Details
CVE-2025-39964	In the Linux kernel, the following vulnerability has been resolved: crypto: af_alg - Disallow concurrent writes in af_alg_sendmsg Issuing two writes to the same af_alg socket is bogus as the data will be interleaved in an unpredictable fashion. Furthermore, concurrent writes may create inconsistencies in the internal socket state. Disallow this by adding a new ctx->write field that indiciates exclusive ownership for writing.	N/A	More Details
CVE-2025-9337	A null pointer dereference has been identified in the AsIO3.sys driver. The vulnerability can be triggered by a specially crafted input, which may lead to a system crash (BSOD). Refer to the 'Security Update for Armoury Crate App' section on the ASUS Security Advisory for more	N/A	More Details

	information.		
CVE-2025-9336	A stack buffer overflow has been identified in the AsIO3.sys driver. This vulnerability can be triggered by input manipulation, may leading to a system crash (BSOD) or other potentially undefined execution. Refer to the 'Security Update for Armoury Crate App' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-11184	Cross-site scripting vulnerability in QGIS QWC2 Registration GUI <=v2025.03.31 allows an authorized attacker to plant arbitrary JavaScript code in the page	N/A	More Details
CVE-2025-11183	Cross-Site Scripting vulnerability in attribute table in QGIS QWC2 <2025.08.14 allows an authorized attacker to plant arbitrary JavaScript code in the page	N/A	More Details
CVE-2025-10720	The WP Private Content Plus through 3.6.2 provides a global content protection feature that requires a password. However, the access control check is based only on the presence of an unprotected client-side cookie. As a result, an unauthenticated attacker can completely bypass the password protection by manually setting the cookie value in their browser.	N/A	More Details
CVE-2025-9968	A link following vulnerability exists in the UnifyScanner component of Armoury Crate. This vulnerability may be triggered by creating a specially crafted junction, potentially leading to local privilege escalation. For more information, please refer to section 'Security Update for Armoury Crate App' in the ASUS Security Advisory.	N/A	More Details
CVE-2025-9265	A broken authorization vulnerability in Kiloview NDI N30 allows a remote unauthenticated attacker to deactivate user verification, giving them access to state changing actions that should only be initiated by administratorsThis issue affects Kiloview NDI N30 and was fixed in Firmware version later than 2.02.0246	N/A	More Details
CVE-2025-8915	Hardcoded TLS private key and certificate in firmware in Kiloview N30 2.02.246 allows malicious adversary to do a Mann-in-the-middle attack via the network	N/A	More Details
CVE-2025-62376	pwn.college DOJO is an education platform for learning cybersecurity. In versions up to and including commit 781d91157cfc234a434d0bab45cbcf97894c642e, the /workspace endpoint contains an improper authentication vulnerability that allows an attacker to access any active Windows VM without proper authorization. The vulnerability occurs in the view_desktop function where the user is retrieved via a URL parameter without verifying that the requester has administrative privileges. An attacker can supply any user ID and arbitrary password in the request parameters to impersonate another user. When requesting a Windows desktop service, the function does not validate the supplied password before generating access credentials, allowing the attacker to obtain an iframe source URL that grants full access to the target user's Windows VM. This impacts all users with active Windows VMs, as an attacker can access and modify data on the Windows machine and in the home directory of the associated Linux machine via the Z: drive. This issue has been patched in commit 467db0b9ea0d9a929dc89b41f6eb59f7cfc68bef. No known workarounds exist.	N/A	More Details