SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06_August_2025

Generated on 06_August_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-2025-54253	Adobe Experience Manager versions 6.5.23 and earlier are affected by a Misconfiguration vulnerability that could result in arbitrary code execution. An attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.	10.0	More Details
CVE-2025-54119	ADOdb is a PHP database class library that provides abstractions for performing queries and managing databases. In versions 5.22.9 and below, improper escaping of a query parameter may allow an attacker to execute arbitrary SQL statements when the code using ADOdb connects to a sqlite3 database and calls the metaColumns(), metaForeignKeys() or metaIndexes() methods with a crafted table name. This is fixed in version 5.22.10. To workaround this issue, only pass controlled data to metaColumns(), metaForeignKeys() and metaIndexes() method's $table parameter.	10.0	More Details
CVE-2025-46093	LiquidFiles before 4.1.2 supports FTP SITE CHMOD for mode 6777 (setuid and setgid), which allows FTPDrop users to execute arbitrary code as root by leveraging the Actionscript feature and the sudoers configuration.	9.9	More Details
CVE-2025-44961	In RUCKUS SmartZone (SZ) before 6.1.2p3 Refresh Build, OS command injection can occur via an IP address field provided by an authenticated user.	9.9	More Details
CVE-2025-7710	The Brave Conversion Engine (PRO) plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 0.7.7. This is due to the plugin not properly restricting a claimed identity while authenticating with Facebook. This makes it possible for unauthenticated attackers to log in as other users, including administrators.	9.8	More Details
CVE-2025-26063	An issue in Intelbras RX1500 v2.2.9 and RX3000 v1.0.11 allows unauthenticated attackers to execute arbitrary code via injecting a crafted payload into the ESSID name when creating a network.	9.8	More Details
CVE-2025-8286	Güralp FMUS series seismic monitoring devices expose an unauthenticated Telnet-based command line interface that could allow an attacker to modify hardware configurations, manipulate data, or factory reset the device.	9.8	More Details

CVE-2025-5954	The Service Finder SMS System plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0. This is due to the plugin not restricting user role selection at the time of registration through the aonesms_fn_savedata_after_signup() function. This makes it possible for unauthenticated attackers to register as an administrator user.	9.8	More Details
CVE-2025-31279	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to fingerprint the user.	9.8	More Details
CVE-2025-8454	It was discovered that uscan, a tool to scan/watch upstream sources for new releases of software, included in devscripts (a collection of scripts to make the life of a Debian Package maintainer easier), skips OpenPGP verification if the upstream source is already downloaded from a previous run even if the verification failed back then.	9.8	More Details
CVE-2019-19144	XML External Entity Injection vulnerability in Quantum DXi6702 2.3.0.3 (11449-53631 Build304) devices via rest/Users?action=authenticate.	9.8	More Details
CVE-2025-50460	A remote code execution (RCE) vulnerability exists in the ms-swift project version 3.3.0 due to unsafe deserialization in tests/run.py using yaml.load() from the PyYAML library (versions = 5.3.1). If an attacker can control the content of the YAML configuration file passed to the --run_config parameter, arbitrary code can be executed during deserialization. This can lead to full system compromise. The vulnerability is triggered when a malicious YAML file is loaded, allowing the execution of arbitrary Python commands such as os.system(). It is recommended to upgrade PyYAML to version 5.4 or higher, and to use yaml.safe_load() to mitigate the issue.	9.8	More Details
CVE-2025-50472	The modelscope/ms-swift library thru 2.6.1 is vulnerable to arbitrary code execution through deserialization of untrusted data within the `load_model_meta()` function of the `ModelFileSystemCache()` class. Attackers can execute arbitrary code and commands by crafting a malicious serialized `.mdl` payload, exploiting the use of `pickle.load()` on data from potentially untrusted sources. This vulnerability allows for remote code execution (RCE) by deceiving victims into loading a seemingly harmless checkpoint during a normal training process, thereby enabling attackers to execute arbitrary code on the targeted machine. Note that the payload file is a hidden file, making it difficult for the victim to detect tampering. More importantly, during the model training process, after the `.mdl` file is loaded and executes arbitrary code, the normal training process remains unaffected'meaning the user remains unaware of the arbitrary code execution.	9.8	More Details
CVE-2025-45150	Insecure permissions in LangChain-ChatGLM-Webui commit ef829 allows attackers to arbitrarily view and download sensitive files via supplying a crafted request.	9.8	More Details
CVE-2025-50870	Institute-of-Current-Students 1.0 is vulnerable to Incorrect Access Control in the mydetailsstudent.php endpoint. The myds GET parameter accepts an email address as input and directly returns the corresponding student's personal information without validating the identity or permissions of the requesting user. This allows any authenticated or unauthenticated attacker to enumerate and retrieve sensitive student details by altering the email value in the request URL, leading to information disclosure.	9.8	More Details
CVE-2025-6077	Partner Software's Partner Software Product and corresponding Partner Web application use the same default username and password for the administrator account across all versions.	9.8	More Details
CVE-2025-51536	Austrian Archaeological Institute (AI) OpenAtlas v8.11.0 as discovered to contain a hardcoded Administrator password.	9.8	More Details
CVE-2025-36594	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.3.0.15, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.60, contain an Authentication Bypass by Spoofing vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass. Remote unauthenticated user can create account that potentially expose customer info, affect system integrity and availability.	9.8	More Details
CVE-2025-50475	An OS command injection vulnerability exists in Russound MBX-PRE-D67F firmware version 3.1.6, allowing unauthenticated attackers to execute arbitrary commands as root via crafted input to the hostname parameter in network configuration requests. This vulnerability stems from improper neutralization of special elements used in an OS command within the network configuration handler, enabling remote code execution with the highest privileges.	9.8	More Details
CVE-2025-	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a command injection		More

51390	vulnerability via the pin parameter in the setWiFiWpsConfig function.	9.8	Details
CVE-2025-52239	An arbitrary file upload vulnerability in ZKEACMS v4.1 allows attackers to execute arbitrary code via a crafted file.	9.8	More Details
CVE-2025-50341	A Boolean-based SQL injection vulnerability was discovered in Axelor 5.2.4 via the _domain parameter. An attacker can manipulate the SQL query logic and determine true/false conditions, potentially leading to data exposure or further exploitation.	9.8	More Details
CVE-2025-51387	The GitKraken Desktop 10.8.0 and 11.1.0 is susceptible to code injection due to misconfigured Electron Fuses. Specifically, the following insecure settings were observed: RunAsNode is enabled and EnableNodeCliInspectArguments is not disabled. These configurations allow the application to be executed in Node.js mode, enabling attackers to pass arguments that result in arbitrary code execution.	9.8	More Details
CVE-2025-27212	An Improper Input Validation in certain UniFi Access devices could allow a Command Injection by a malicious actor with access to UniFi Access management network. Affected Products: UniFi Access Reader Pro (Version 2.14.21 and earlier) UniFi Access G2 Reader Pro (Version 1.10.32 and earlier) UniFi Access G3 Reader Pro (Version 1.10.30 and earlier) UniFi Access Intercom (Version 1.7.28 and earlier) UniFi Access G3 Intercom (Version 1.7.29 and earlier) UniFi Access Intercom Viewer (Version 1.3.20 and earlier) Mitigation: Update UniFi Access Reader Pro Version 2.15.9 or later Update UniFi Access G2 Reader Pro Version 1.11.23 or later Update UniFi Access G3 Reader Pro Version 1.11.22 or later Update UniFi Access Intercom Version 1.8.22 or later Update UniFi Access G3 Intercom Version 1.8.22 or later Update UniFi Access Intercom Viewer Version 1.4.39 or later	9.8	More Details
CVE-2025-54802	pyLoad is the free and open-source Download Manager written in pure Python. In versions 0.5.0b3.dev89 and below, there is an opportunity for path traversal in pyLoad-ng CNL Blueprint via package parameter, allowing Arbitrary File Write which leads to Remote Code Execution (RCE). The addcrypted endpoint in pyload-ng suffers from an unsafe path construction vulnerability, allowing unauthenticated attackers to write arbitrary files outside the designated storage directory. This can be abused to overwrite critical system files, including cron jobs and systemd services, leading to privilege escalation and remote code execution as root. This issue is fixed in version 0.5.0b3.dev90.	9.8	More Details
CVE-2025-50706	An issue in thinkphp v.5.1 allows a remote attacker to execute arbitrary code via the routecheck function	9.8	More Details
CVE-2025-50707	An issue in thinkphp3 v.3.2.5 allows a remote attacker to execute arbitrary code via the index.php component	9.8	More Details
CVE-2025-46658	An issue was discovered in ExonautWeb in 4C Strategies Exonaut 21.6. There are verbose error messages.	9.8	More Details
CVE-2025-26062	An access control issue in Intelbras RX1500 v2.2.9 and RX3000 v1.0.11 allows unauthenticated attackers to access the router's settings file and obtain potentially sensitive information from the current settings.	9.8	More Details
CVE-2025-5947	The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via authentication bypass in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's cookie value prior to logging them in through the service_finder_switch_back() function. This makes it possible for unauthenticated attackers to login as any user including admins.	9.8	More Details
CVE-2025-43237	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6. An app may be able to cause unexpected system termination.	9.8	More Details
CVE-2025-43193	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to cause a denial-of-service.	9.8	More Details
CVE-2025-43198	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to access protected user data.	9.8	More Details
CVE-2025-43199	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. A malicious app may be able to gain root privileges.	9.8	More Details

CVE-2025-43209	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sonoma 14.7.7, watchOS 11.6, visionOS 2.6, macOS Ventura 13.7.7. Processing maliciously crafted web content may lead to an unexpected Safari crash.	9.8	More Details
CVE-2025-43220	This issue was addressed with improved validation of symlinks. This issue is fixed in iPadOS 17.7.9, macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access protected user data.	9.8	More Details
CVE-2025-43192	A configuration issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. Account-driven User Enrollment may still be possible with Lockdown Mode turned on.	9.8	More Details
CVE-2025-43189	This issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. A malicious app may be able to read kernel memory.	9.8	More Details
CVE-2025-43222	A use-after-free issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6, iPadOS 17.7.9, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An attacker may be able to cause unexpected app termination.	9.8	More Details
CVE-2025-43232	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to bypass certain Privacy preferences.	9.8	More Details
CVE-2025-43233	This issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. A malicious app acting as a HTTPS proxy could get access to sensitive user data.	9.8	More Details
CVE-2025-43234	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 11.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sequoia 15.6, visionOS 2.6. Processing a maliciously crafted texture may lead to unexpected app termination.	9.8	More Details
CVE-2025-43194	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to modify protected parts of the file system.	9.8	More Details
CVE-2025-43253	This issue was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. A malicious app may be able to launch arbitrary binaries on a trusted device.	9.8	More Details
CVE-2025-43243	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to modify protected parts of the file system.	9.8	More Details
CVE-2025-43244	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to cause unexpected system termination.	9.8	More Details
CVE-2025-43186	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sequoia 15.6, macOS Sonoma 14.7.7, visionOS 2.6, macOS Ventura 13.7.7. Parsing a file may lead to an unexpected app termination.	9.8	More Details
CVE-2025-43245	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access protected user data.	9.8	More Details
CVE-2025-43261	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	9.8	More Details
CVE-2025-43184	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.7.7, macOS Ventura 13.7.7, macOS Sequoia 15.4. A shortcut may be able to bypass sensitive Shortcuts app settings.	9.8	More Details
CVE-2025-43275	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	9.8	More Details
	LinuxServer.io heimdall 2.6.3-ls307 contains a vulnerability in how it handles user-supplied HTTP headers, specifically `X-Forwarded-Host` and `Referer`. An unauthenticated remote attacker can		

CVE-2025-50578	manipulate these headers to perform Host Header Injection and Open Redirect attacks. This allows the loading of external resources from attacker-controlled domains and unintended redirection of users, potentially enabling phishing, UI redress, and session theft. The vulnerability exists due to insufficient validation and trust of untrusted input, affecting the integrity and trustworthiness of the application.	9.8	More Details
CVE-2025-46811	A Missing Authentication for Critical Function vulnerability in SUSE Manager allows anyone with access to the websocket at /rhn/websocket/minion/remote-commands to execute arbitrary commands as root. This issue affects Container suse/manager/5.0/x86_64/server:5.0.5.7.30.1: from ? before 0.3.7-150600.3.6.2; Container suse/manager/5.0/x86_64/server:5.0.5.7.30.1: from ? before 5.0.14-150600.4.17.1; Container suse/manager/5.0/x86_64/server:5.0.5.7.30.1: from ? before 5.0.14-150600.4.17.1; Image SLES15-SP4-Manager-Server-4-3-BYOS: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-Azure: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-Azure: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-EC2: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-EC2: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-GCE: from ? before 4.3.33-150400.3.55.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-GCE: from ? before 4.3.33-150400.3.55.2; SUSE Manager Server Module 4.3: from ? before 0.3.7-150400.3.39.4; SUSE Manager Server Module 4.3: from ? before 4.3.33-150400.3.55.2; SUSE Manager Server Module 4.3: from ? before 4.3.33-150400.3.55.2.	9.8	More Details
CVE-2025-50754	Unisite CMS version 5.0 contains a stored Cross-Site Scripting (XSS) vulnerability in the "Report" functionality. A malicious script submitted by an attacker is rendered in the admin panel when viewed by an administrator. This allows attackers to hijack the admin session and, by leveraging the template editor, upload and execute a PHP web shell on the server, leading to full remote code execution.	9.6	More Details
CVE-2025-54982	An improper verification of cryptographic signature in Zscaler's SAML authentication mechanism on the server-side allowed an authentication abuse.	9.6	More Details
CVE-2025-54948	A vulnerability in Trend Micro Apex One (on-premise) management console could allow a pre-authenticated remote attacker to upload malicious code and execute commands on affected installations.	9.4	More Details
CVE-2025-54987	A vulnerability in Trend Micro Apex One (on-premise) management console could allow a pre-authenticated remote attacker to upload malicious code and execute commands on affected installations. This vulnerability is essentially the same as CVE-2025-54948 but targets a different CPU architecture.	9.4	More Details
CVE-2025-54574	Squid is a caching proxy for the Web. In versions 6.3 and below, Squid is vulnerable to a heap buffer overflow and possible remote code execution attack when processing URN due to incorrect buffer management. This has been fixed in version 6.4. To work around this issue, disable URN access permissions.	9.3	More Details
CVE-2025-31281	An input validation issue was addressed with improved memory handling. This issue is fixed in visionOS 2.6, tvOS 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6. Processing a maliciously crafted file may lead to unexpected app termination.	9.1	More Details
CVE-2025-49084	CVE-2025-49084 is a vulnerability in the management console of Absolute Secure Access prior to version 13.56. Attackers with administrative access can overwrite policy rules without the requisite permissions. The attack complexity is low, attack requirements are present, privileges required are high and no user interaction is required. There is no impact to confidentiality, the impact to integrity is low, and there is no impact to availability. The impact to confidentiality and availability of subsequent systems is high and the impact to the integrity of subsequent systems is low.	9.1	More Details
CVE-2025-31229	A logic issue was addressed with improved checks. This issue is fixed in iOS 18.6 and iPadOS 18.6. Passcode may be read aloud by VoiceOver.	9.1	More Details
CVE-2025-51535	Austrian Archaeological Institute (AI) OpenAtlas v8.11.0 as discovered to contain a SQL injection vulnerability.	9.1	More Details
	OAuth2-Proxy is an open-source tool that can act as either a standalone reverse proxy or a middleware component integrated into existing reverse proxy or load balancer setups. In versions 7.10.0 and below, oauth2-proxy deployments are vulnerable when using the skip_auth_routes configuration option with regex patterns. Attackers can bypass authentication by crafting URLs		

CVE-2025-54576	with query parameters that satisfy configured regex patterns, allowing unauthorized access to protected resources. The issue stems from skip_auth_routes matching against the full request URI. Deployments using skip_auth_routes with regex patterns containing wildcards or broad matching patterns are most at risk. This issue is fixed in version 7.11.0. Workarounds include: auditing all skip_auth_routes configurations for overly permissive patterns, replacing wildcard patterns with exact path matches where possible, ensuring regex patterns are properly anchored (starting with ^ and ending with $), or implementing custom validation that strips query parameters before regex matching.	9.1	More Details
CVE-2025-6205	A missing authorization vulnerability affecting DELMIA Apriso from Release 2020 through Release 2025 could allow an attacker to gain privileged access to the application.	9.1	More Details
CVE-2025-6000	A privileged Vault operator within the root namespace with write permission to {{sys/audit}} may obtain code execution on the underlying host if a plugin directory is set in Vault's configuration. Fixed in Vault Community Edition 1.20.1 and Vault Enterprise 1.20.1, 1.19.7, 1.18.12, and 1.16.23.	9.1	More Details
CVE-2025-52390	Saurus CMS Community Edition since commit d886e5b0 (2010-04-23) is vulnerable to a SQL Injection vulnerability in the \`prepareSearchQuery()\` method in \`FulltextSearch.class.php\`. The application directly concatenates user-supplied input (\`$search_word\`) into SQL queries without sanitization, allowing attackers to manipulate the SQL logic and potentially extract sensitive information or escalate their privileges.	9.1	More Details
CVE-2025-43273	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.6. A sandboxed process may be able to circumvent sandbox restrictions.	9.1	More Details
CVE-2025-54430	dedupe is a python library that uses machine learning to perform fuzzy matching, deduplication and entity resolution quickly on structured data. Before commit 3f61e79, a critical severity vulnerability has been identified within the .github/workflows/benchmark-bot.yml workflow, where a issue_comment can be triggered using the @benchmark body. This workflow is susceptible to exploitation as it checkout the ${{ github.event.issue.number }}, which correspond to the branch of the PR manipulated by potentially malicious actors, and where untrusted code may be executed. Running untrusted code may lead to the exfiltration of GITHUB_TOKEN, which in this workflow has write permissions on most of the scopes - in particular the contents one - and could lead to potential repository takeover. This is fixed by commit 3f61e79.	9.1	More Details
CVE-2025-44963	RUCKUS Network Director (RND) before 4.5 allows spoofing of an administrator JWT by an attacker who knows the hardcoded value of a certain secret key.	9.0	More Details
CVE-2025-44954	RUCKUS SmartZone (SZ) before 6.1.2p3 Refresh Build has a hardcoded SSH private key for a root-equivalent user account.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-54351	In iperf before 3.19.1, net.c has a buffer overflow when --skip-rx-copy is used (for MSG_TRUNC in recv).	8.9	More Details
CVE-2025-6754	The SEO Metrics plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization checks in both the seo_metrics_handle_connect_button_click() AJAX handler and the seo_metrics_handle_custom_endpoint() function in versions 1.0.5 through 1.0.15. Because the AJAX action only verifies a nonce, without checking the caller's capabilities, a subscriber-level user can retrieve the token and then access the custom endpoint to obtain full administrator cookies.	8.8	More Details
CVE-2025-50572	An issue was discovered in Archer Technology RSA Archer 6.11.00204.10014 allowing attackers to execute arbitrary code via crafted system inputs that would be exported into the CSV and be executed after the user opened the file with compatible applications.	8.8	More Details
CVE-2025-26332	TechAdvisor versions 2.6 through 3.37-30 for Dell XtremIO X2, contain(s) an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	8.8	More Details
	Dell XtremIO, version(s) 6.4.0-22, contain(s) an Insertion of Sensitive Information into Log File		

CVE-2025-30105	vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	8.8	More Details
CVE-2025-8322	The e-School from Ventem has a Missing Authorization vulnerability, allowing remote attackers with regular privilege to access administrator functions, including creating, modifying, and deleting accounts. They can even escalate any account to system administrator privilege.	8.8	More Details
CVE-2025-8292	Use after free in Media Stream in Google Chrome prior to 138.0.7204.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-6076	Partner Software's Partner Software application and Partner Web application do not sanitize files uploaded on the "reports" tab, allowing an authenticated attacker to upload a malicious file and compromise the device. By default, the software runs as SYSTEM, heightening the severity of the vulnerability.	8.8	More Details
CVE-2025-8109	Software installed and run as a non-privileged user may conduct ptrace system calls to issue writes to GPU origin read only memory.	8.8	More Details
CVE-2025-8323	The e-School from Ventem has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	8.8	More Details
CVE-2025-44955	RUCKUS Network Director (RND) before 4.5 allows jailed users to obtain root access vis a weak, hardcoded password.	8.8	More Details
CVE-2025-20702	In the Airoha Bluetooth audio SDK, there is a possible unauthorized access to the RACE protocol. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-31278	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, iPadOS 17.7.9, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-31277	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-20701	In the Airoha Bluetooth audio SDK, there is a possible way to pair Bluetooth audio device without user consent. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-31273	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-20700	In the Airoha Bluetooth audio SDK, there is a possible permission bypass that allows access critical data of RACE protocol through Bluetooth LE GATT service. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2025-7847	The AI Engine plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the rest_simpleFileUpload() function in versions 2.9.3 and 2.9.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server when the REST API is enabled, which may make remote code execution possible.	8.8	More Details
CVE-2025-43270	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may gain unauthorized access to Local Network.	8.8	More Details
CVE-	TrustedFirmware-M (aka Trusted Firmware for M profile Arm CPUs) before 2.1.3 and 2.2.x before 2.2.1 lacks length validation during a firmware upgrade. While processing a new image, the Firmware Upgrade (FWU) module does not validate the length field of the Type-Length-Value (TLV) structure for dependent components against the maximum allowed size. If the length specified in the		More

2025-53022	TLV exceeds the size of the buffer allocated on the stack, the FWU module will overwrite the buffer (and potentially other stack data) with the TLV's value content. An attacker could exploit this by crafting a malicious TLV entry in the unprotected section of the MCUBoot upgrade image. By setting the length field to exceed the expected structure size, the attacker can manipulate the stack memory of the system during the upgrade process.	8.6	Details
CVE-2025-54254	Adobe Experience Manager versions 6.5.23 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files on the local file system. Exploitation of this issue does not require user interaction.	8.6	More Details
CVE-2025-50850	An issue was discovered in CS Cart 4.18.3 allows the vendor login functionality lacks essential security controls such as CAPTCHA verification and rate limiting. This allows an attacker to systematically attempt various combinations of usernames and passwords (brute-force attack) to gain unauthorized access to vendor accounts. The absence of any blocking mechanism makes the login endpoint susceptible to automated attacks.	8.6	More Details
CVE-2025-44643	Certain Draytek products are affected by Insecure Configuration. This affects AP903 v1.4.18 and AP912C v1.4.9 and AP918R v1.4.9. The setting of the password property in the ripd.conf configuration file sets a hardcoded weak password, posing a security risk. An attacker with network access could exploit this to gain unauthorized control over the routing daemon, potentially altering network routes or intercepting traffic.	8.6	More Details
CVE-2025-44960	RUCKUS SmartZone (SZ) before 6.1.2p3 Refresh Build allows OS command injection via a certain parameter in an API route.	8.5	More Details
CVE-2025-44957	Ruckus SmartZone (SZ) before 6.1.2p3 Refresh Build allows authentication bypass via a valid API key and crafted HTTP headers.	8.5	More Details
CVE-2025-54135	Cursor is a code editor built for programming with AI. Cursor allows writing in-workspace files with no user approval in versions below 1.3.9, If the file is a dotfile, editing it requires approval but creating a new one doesn't. Hence, if sensitive MCP files, such as the .cursor/mcp.json file don't already exist in the workspace, an attacker can chain a indirect prompt injection vulnerability to hijack the context to write to the settings file and trigger RCE on the victim without user approval. This is fixed in version 1.3.9.	8.5	More Details
CVE-2025-51726	CyberGhostVPNSetup.exe (Windows installer) is signed using the weak cryptographic hash algorithm SHA-1, which is vulnerable to collision attacks. This allows a malicious actor to craft a fake installer with a forged SHA-1 certificate that may still be accepted by Windows signature verification mechanisms, particularly on systems without strict SmartScreen or trust policy enforcement. Additionally, the installer lacks High Entropy Address Space Layout Randomization (ASLR), as confirmed by BinSkim (BA2015 rule) and repeated WinDbg analysis. The binary consistently loads into predictable memory ranges, increasing the success rate of memory corruption exploits. These two misconfigurations, when combined, significantly lower the bar for successful supply-chain style attacks or privilege escalation through fake installers.	8.4	More Details
CVE-2025-26476	Dell ECS versions prior to 3.8.1.5/ ObjectScale version 4.0.0.0, contain a Use of Hard-coded Cryptographic Key vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	8.4	More Details
CVE-2025-21120	Dell Avamar, versions prior to 19.12 with patch 338905, excluding version 19.10SP1 with patch 338904, contains a Trusting HTTP Permission Methods on the Server-Side vulnerability in Security. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	8.3	More Details
CVE-2025-41659	A low-privileged attacker can remotely access the PKI folder of the CODESYS Control runtime system and thus read and write certificates and its keys. This allows sensitive data to be extracted or to accept certificates as trusted. Although all services remain available, only unencrypted communication is possible if the certificates are deleted.	8.3	More Details
CVE-2025-4425	The vulnerability was identified in the code developed specifically for Lenovo. Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the vulnerability. https://support.lenovo.com/us/en/product_security/home	8.2	More Details
CVE-2025-	The vulnerability was identified in the code developed specifically for Lenovo. Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the	8.2	More Details

4423	vulnerability. https://support.lenovo.com/us/en/product_security/home		
CVE-2025-4422	The vulnerability was identified in the code developed specifically for Lenovo. Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the vulnerability. https://support.lenovo.com/us/en/product_security/home	8.2	More Details
CVE-2025-4421	The vulnerability was identified in the code developed specifically for Lenovo. Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the vulnerability. https://support.lenovo.com/us/en/product_security/home	8.2	More Details
CVE-2025-52187	GetProjectsIdea Create School Management System 1.0 is vulnerable to Cross Site Scripting (XSS) in my_profile_update_form1.php.	8.2	More Details
CVE-2025-45620	An issue in Aver PTC310UV2 v.0.1.0000.59 allows a remote attacker to obtain sensitive information via a crafted request	8.1	More Details
CVE-2025-51534	A cross-site scripting (XSS) vulnerability in Austrian Archaeological Institute (AI) OpenAtlas v8.11.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name field.	8.1	More Details
CVE-2024-48916	Ceph is a distributed object, block, and file storage platform. In versions 19.2.3 and below, it is possible to send an JWT that has "none" as JWT alg. And by doing so the JWT signature is not checked. The vulnerability is most likely in the RadosGW OIDC provider. As of time of publication, a known patched version has yet to be published.	8.1	More Details
CVE-2025-54955	OpenNebula Community Edition (CE) before 7.0.0 and Enterprise Edition (EE) before 6.10.3 have a critical FireEdge race condition that can lead to full account takeover. By exploiting this, an unauthenticated attacker can obtain a valid JSON Web Token (JWT) belonging to a legitimate user without knowledge of their credentials.	8.1	More Details
CVE-2025-7443	The BerqWP – Automated All-In-One Page Speed Optimization for Core Web Vitals, Cache, CDN, Images, CSS, and JavaScript plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation via the store_javascript_cache.php file in all versions up to, and including, 2.2.42. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.1	More Details
CVE-2025-54424	1Panel is a web interface and MCP Server that manages websites, files, containers, databases, and LLMs on a Linux server. In versions 2.0.5 and below, the HTTPS protocol used for communication between the Core and Agent endpoints has incomplete certificate verification during certificate validation, leading to unauthorized interface access. Due to the presence of numerous command execution or high-privilege interfaces in 1Panel, this results in Remote Code Execution (RCE). This is fixed in version 2.0.6. The CVE has been translated from Simplified Chinese using GitHub Copilot.	8.1	More Details
CVE-2025-50849	CS Cart 4.18.3 is vulnerable to Insecure Direct Object Reference (IDOR). The user profile functionality allows enabling or disabling stickers through a parameter (company_id) sent in the request. However, this operation is not properly validated on the server side. An authenticated user can manipulate the request to target other users' accounts and toggle the sticker setting by modifying the company_id or other object identifiers.	8.0	More Details
CVE-2025-6204	An Improper Control of Generation of Code (Code Injection) vulnerability affecting DELMIA Apriso from Release 2020 through Release 2025 could allow an attacker to execute arbitrary code.	8.0	More Details
CVE-2025-52289	A Broken Access Control vulnerability in MagnusBilling v7.8.5.3 allows newly registered users to gain escalated privileges by sending a crafted request to /mbilling/index.php/user/save to set their account status fom "pending" to "active" without requiring administrator approval.	8.0	More Details
CVE-2025-23276	NVIDIA Installer for Windows contains a vulnerability where an attacker may be able to escalate privileges. A successful exploit of this vulnerability may lead to escalation of privileges, denial of service, code execution, information disclosure and data tampering.	7.8	More Details
CVE-2025-23283	NVIDIA vGPU software for Linux-style hypervisors contains a vulnerability in the Virtual GPU Manager, where a malicious guest could cause stack buffer overflow. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.8	More Details
CVE-	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious guest		

2025-23284	could cause a stack buffer overflow. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, or data tampering.	7.8	More Details
CVE-2025-30099	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A low privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	7.8	More Details
CVE-2025-50777	The firmware of the AZIOT 2MP Full HD Smart Wi-Fi CCTV Home Security Camera (version V1.00.02) contains an Incorrect Access Control vulnerability that allows local attackers to gain root shell access. Once accessed, the device exposes critical data including Wi-Fi credentials and ONVIF service credentials stored in plaintext, enabling further compromise of the network and connected systems.	7.8	More Details
CVE-2025-36607	Dell Unity, version(s) 5.5 and prior, contain(s) an OS Command Injection Vulnerability in its svc_nas utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	7.8	More Details
CVE-2025-36606	Dell Unity, version(s) 5.5 and prior, contain(s) an OS Command Injection Vulnerability in its svc_nfssupport utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	7.8	More Details
CVE-2025-43277	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.6 and iPadOS 18.6, watchOS 11.6, macOS Sequoia 15.6, tvOS 18.6, visionOS 2.6. Processing a maliciously crafted audio file may lead to memory corruption.	7.8	More Details
CVE-2025-24119	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.3, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	7.8	More Details
CVE-2025-31243	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7.7, macOS Ventura 13.7.7, macOS Sequoia 15.6. An app may be able to gain root privileges.	7.8	More Details
CVE-2025-43188	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6. A malicious app may be able to gain root privileges.	7.8	More Details
CVE-2025-41698	A low privileged local attacker can interact with the affected service although user-interaction should not be allowed.	7.8	More Details
CVE-2025-52327	SQL Injection vulnerability in Restaurant Order System 1.0 allows a local attacker to obtain sensitive information via the payment.php file	7.8	More Details
CVE-2025-54564	uploadsm in ChargePoint Home Flex 5.5.4.13 does not validate a user-controlled string for bz2 decompression, which allows command execution as the nobody user.	7.8	More Details
CVE-2025-31280	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted file may lead to heap corruption.	7.8	More Details
CVE-2025-43256	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to gain root privileges.	7.8	More Details
CVE-2025-43248	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. A malicious app may be able to gain root privileges.	7.8	More Details
CVE-2025-43196	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to gain root privileges.	7.8	More Details
CVE-			

2025-43249	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to gain root privileges.	7.8	More Details
CVE-2025-52361	Insecure permissions in the script /etc/init.d/lighttpd in AK-Nord USB-Server-LXL Firmware v0.0.16 Build 2023-03-13 allows a locally authenticated low-privilege user to execute arbitrary commands with root privilege via editing this script which is executed with root-privileges on any interaction and on every system boot.	7.8	More Details
CVE-2025-53394	Paramount Macrium Reflect through 2025-06-26 allows attackers to execute arbitrary code with administrator privileges via a crafted .mrimgx or .mrbax backup file and a renamed executable placed in the same directory. When a user with administrative privileges opens the crafted backup file and proceeds to mount it, Reflect launches the renamed executable (e.g., explorer.exe), which is under attacker control. This occurs because of insufficient validation of companion files referenced during backup mounting.	7.7	More Details
CVE-2025-53944	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents. In v0.6.15 and below, the external API's get_graph_execution_results endpoint has an authorization bypass vulnerability. While it correctly validates user access to the graph_id, it fails to verify ownership of the graph_exec_id parameter, allowing authenticated users to access any execution results by providing arbitrary execution IDs. The internal API implements proper validation for both parameters. This is fixed in v0.6.16.	7.7	More Details
CVE-2025-53395	Paramount Macrium Reflect through 2025-06-26 allows local attackers to execute arbitrary code with administrator privileges via a crafted .mrimgx backup file and a malicious VSSSvr.dll located in the same directory. When a user with administrative privileges mounts a backup by opening the .mrimgx file, Reflect loads the attacker's VSSSvr.dll after the mount completes. This occurs because of untrusted DLL search path behavior in ReflectMonitor.exe.	7.7	More Details
CVE-2025-54780	The glpi-screenshot-plugin allows users to take screenshots or screens recording directly from GLPI. In versions below 2.0.2, authenticated user can use the /ajax/screenshot.php endpoint to leak files from the system or use PHP wrappers. This is fixed in version 2.0.2.	7.7	More Details
CVE-2025-52203	A stored cross-site scripting (XSS) vulnerability exists in DevaslanPHP project-management v1.2.4. The vulnerability resides in the Ticket Name field, which fails to properly sanitize user-supplied input. An authenticated attacker can inject malicious JavaScript payloads into this field, which are subsequently stored in the database. When a legitimate user logs in and is redirected to the Dashboard panel "automatically upon authentication the malicious script executes in the user's browser context.	7.6	More Details
CVE-2025-51503	A Stored Cross-Site Scripting (XSS) vulnerability in Microweber CMS 2.0 allows attackers to inject malicious scripts into user profile fields, leading to arbitrary JavaScript execution in admin browsers.	7.6	More Details
CVE-2025-51504	Microweber CMS 2.0 is vulnerable to Cross Site Scripting (XSS)in the /projects/profile, homepage endpoint via the last name field.	7.6	More Details
CVE-2025-41691	An unauthenticated remote attacker may trigger a NULL pointer dereference in the affected CODESYS Control runtime systems by sending specially crafted communication requests, potentially leading to a denial-of-service (DoS) condition.	7.5	More Details
CVE-2025-43227	This issue was addressed through improved state management. This issue is fixed in Safari 18.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may disclose sensitive user information.	7.5	More Details
CVE-2025-54581	vproxy is an HTTP/HTTPS/SOCKS5 proxy server. In versions 2.3.3 and below, untrusted data is extracted from the user-controlled HTTP Proxy-Authorization header and passed to Extension::try_from and flows into parse_ttl_extension where it is parsed as a TTL value. If an attacker supplies a TTL of zero (e.g. by using a username such as 'configuredUser-ttl-0'), the modulo operation 'timestamp % ttl' will cause a division by zero panic, causing the server to crash causing a denial-of-service. This is fixed in version 2.4.0.	7.5	More Details
CVE-2025-54868	LibreChat is a ChatGPT clone with additional features. In versions 0.0.6 through 0.7.7-rc1, an exposed testing endpoint allows reading arbitrary chats directly from the Meilisearch engine. The endpoint /api/search/test allows for direct access to stored chats in the Meilisearch engine without proper access control. This results in the ability to read chats from arbitrary users. This issue is fixed in version 0.7.7.	7.5	More Details

CVE-2025-38741	Dell Enterprise SONiC OS, version 4.5.0, contains a cryptographic key vulnerability in SSH. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to unauthorized access to communication.	7.5	More Details
CVE-2025-24853	A carefully crafted request when creating a header link using the wiki markup syntax, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Further research by the JSPWiki team showed that the markdown parser allowed this kind of attack too. Apache JSPWiki users should upgrade to 2.12.3 or later.	7.5	More Details
CVE-2023-32256	A flaw was found in the Linux kernel's ksmbd component. A race condition between smb2 close operation and logoff in multichannel connections could result in a use-after-free issue.	7.5	More Details
CVE-2025-2813	An unauthenticated remote attacker can cause a Denial of Service by sending a large number of requests to the http service on port 80.	7.5	More Details
CVE-2025-43223	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.7, iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6, macOS Sonoma 14.7.7, watchOS 11.6, macOS Sequoia 15.6, tvOS 18.6, visionOS 2.6. A non-privileged user may be able to modify restricted network settings.	7.5	More Details
CVE-2025-53544	Trilium Notes is an open-source, cross-platform hierarchical note taking application with focus on building large personal knowledge bases. In versions below 0.97.0, a brute-force protection bypass in the initial sync seed retrieval endpoint allows unauthenticated attackers to guess the login password without triggering rate limiting. Trilium is a single-user app without a username requirement, and brute-force protection bypass makes exploitation much more feasible. Multiple features provided by Trilium (e.g. MFA, share notes, custom request handler) indicate that Trilium can be exposed to the internet. This is fixed in version 0.97.0.	7.5	More Details
CVE-2025-29745	A vulnerability affecting the scanning module in Emsisoft Anti-Malware prior to 2024.12 allows attackers on a remote server to obtain Net-NTLMv2 hash information via a specially created A2S (Emsisoft Custom Scan) extension file.	7.5	More Details
CVE-2025-51628	Insecure Direct Object Reference (IDOR) vulnerability in PdfHandler component in Agenzia Impresa Eccobook v2.81.1 and below allows unauthenticated attackers to read confidential documents via the DocumentoId parameter.	7.5	More Details
CVE-2025-54796	Copyparty is a portable file server. Versions prior to 1.18.9, the filter parameter for the "Recent Uploads" page allows arbitrary RegExes. If this feature is enabled (which is the default), an attacker can craft a filter which deadlocks the server. This is fixed in version 1.18.9.	7.5	More Details
CVE-2025-24224	The issue was addressed with improved checks. This issue is fixed in tvOS 18.5, iOS 18.5 and iPadOS 18.5, iPadOS 17.7.9, macOS Sequoia 15.5, watchOS 11.5, visionOS 2.5, macOS Ventura 13.7.7. A remote attacker may be able to cause unexpected system termination.	7.5	More Details
CVE-2025-5061	The WP Import Export Lite plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'wpie_parse_upload_data' function in all versions up to, and including, 3.9.29. This makes it possible for authenticated attackers, with Subscriber-level access and above, and permissions granted by an Administrator, to upload arbitrary files on the affected site's server which may make remote code execution possible. The vulnerability was partially patched in version 3.9.29.	7.5	More Details
CVE-2025-27211	An Improper Input Validation in EdgeMAX EdgeSwitch (Version 1.10.4 and earlier) could allow a Command Injection by a malicious actor with access to EdgeSwitch adjacent network.	7.5	More Details
CVE-2025-6207	The WP Import Export Lite plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'wpie_tempalte_import' function in all versions up to, and including, 3.9.28. This makes it possible for authenticated attackers, with Subscriber-level access and above, and permissions granted by an Administrator, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.5	More Details
CVE-2025-54130	Cursor is a code editor built for programming with AI. Cursor allows writing in-workspace files with no user approval in versions less than 1.3.9. If the file is a dotfile, editing it requires approval but creating a new one doesn't. Hence, if sensitive editor files, such as the .vscode/settings.json file don't already exist in the workspace, an attacker can chain a indirect prompt injection vulnerability to hijack the context to write to the settings file and trigger RCE on the victim without user approval. This is fixed in version 1.3.9.	7.5	More Details

CVE-2025-43978	Jointelli 5G CPE 21H01 firmware JY_21H01_A3_v1.36 devices allow (blind) OS command injection. Multiple endpoints are vulnerable, including /ubus/?flag=set_WPS_pin and /ubus/?flag=netAppStar1 and /ubus/?flag=set_wifi_cfgs. This allows an authenticated attacker to execute arbitrary OS commands with root privileges via crafted inputs to the SSID, WPS, Traceroute, and Ping fields.	7.4	More Details
CVE-2025-43979	An issue was discovered on FIRSTNUM JC21A-04 devices through 2.01ME/FN that allows authenticated attackers to execute arbitrary OS system commands with root privileges via crafted payloads to the xml_action.cgi?method= endpoint.	7.4	More Details
CVE-2025-2824	IBM Operational Decision Manager 8.11.0.1, 8.11.1.0, 8.12.0.1, 9.0.0.1, and 9.5.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	7.4	More Details
CVE-2025-8374	A vulnerability was found in code-projects Vehicle Management 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /addcompany.php. The manipulation of the argument company leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8330	A vulnerability has been found in code-projects Vehicle Management 1.0 and classified as critical. This vulnerability affects unknown code of the file /edit1.php. The manipulation of the argument sno leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8438	A vulnerability classified as critical was found in code-projects Wazifa System 1.0. This vulnerability affects unknown code of the file /controllers/postpublish.php. The manipulation of the argument post leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8375	A vulnerability was found in code-projects Vehicle Management 1.0. It has been rated as critical. This issue affects some unknown processing of the file /addvehicle.php. The manipulation of the argument vehicle leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8334	A vulnerability was found in Campcodes Online Recruitment Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/ajax.php?action=delete_recruitment_status. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-26065	A cross-site scripting (XSS) vulnerability in Intelbras RX1500 v2.2.9 and RX3000 v1.0.11 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name of a visiting Wi-Fi network.	7.3	More Details
CVE-2025-8437	A vulnerability classified as critical has been found in code-projects Kitchen Treasure 1.0. This affects an unknown part of the file /userregistration.php. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8494	A vulnerability, which was classified as critical, has been found in code-projects Intern Membership Management System 1.0. This issue affects some unknown processing of the file /admin/delete_student.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8333	A vulnerability was found in code-projects Online Farm System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /categoryvalue.php. The manipulation of the argument Value leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8331	A vulnerability was found in code-projects Online Farm System 1.0 and classified as critical. This issue affects some unknown processing of the file /forgot_pass.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-	A vulnerability was found in code-projects Online Farm System 1.0. It has been classified as critical. Affected is an unknown function of the file /register.php. The manipulation of the argument	7.3	More

8332	Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		Details
CVE-2025-29556	ExaGrid EX10 6.3 - 7.0.1.P08 is vulnerable to Incorrect Access Control. Since version 6.3, ExaGrid enforces restrictions preventing users with the Admin role from creating or modifying users with the Security Officer role without approval. However, a flaw in the account creation process allows an attacker to bypass these restrictions via API request manipulation. An attacker with an Admin access can intercept and modify the API request during user creation, altering the parameters to assign the new account to the ExaGrid Security Officers group without the required approval.	7.3	More Details
CVE-2025-8336	A vulnerability classified as critical was found in Campcodes Online Recruitment Management System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=save_user. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-36604	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution.	7.3	More Details
CVE-2025-8373	A vulnerability was found in code-projects Vehicle Management 1.0. It has been classified as critical. This affects an unknown part of the file /print.php. The manipulation of the argument sno leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8372	A vulnerability was found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/update_s7.php. The manipulation of the argument credits leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8436	A vulnerability was found in projectworlds Online Admission System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /viewdoc.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8339	A vulnerability was found in code-projects Intern Membership Management System 1.0. It has been classified as critical. This affects an unknown part of the file /student_login.php. The manipulation of the argument user_name/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8435	A vulnerability was found in code-projects Online Movie Streaming 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin-control.php. The manipulation of the argument ID leads to missing authorization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8434	A vulnerability was found in code-projects Online Movie Streaming 1.0. It has been classified as critical. Affected is an unknown function of the file /admin.php. The manipulation of the argument ID leads to missing authorization. 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-2025-8495	A vulnerability, which was classified as critical, was found in code-projects Intern Membership Management System 1.0. Affected is an unknown function of the file /admin/edit_admin_query.php. The manipulation of the argument Username 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-2025-8371	A vulnerability has been found in code-projects Exam Form Submission 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/update_s5.php. The manipulation of the argument credits leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8496	A vulnerability has been found in projectworlds Online Admission System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /viewform.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8497	A vulnerability was found in code-projects Online Medicine Guide 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /cusfindphar2.php. The manipulation of the argument Search leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE-2025-8498	A vulnerability was found in code-projects Online Medicine Guide 1.0. It has been classified as critical. This affects an unknown part of the file /cart/index.php. The manipulation of the argument uname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8499	A vulnerability was found in code-projects Online Medicine Guide 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cusfindambulence2.php. The manipulation of the argument Search leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8503	A vulnerability, which was classified as critical, has been found in code-projects Online Medicine Guide 1.0. Affected by this issue is some unknown functionality of the file /adaddmed.php. The manipulation of the argument mname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8338	A vulnerability was found in projectworlds Online Admission System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /adminac.php. The manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8493	A vulnerability classified as critical was found in code-projects Intern Membership Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_student_query.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8439	A vulnerability, which was classified as critical, has been found in code-projects Wazifa System 1.0. This issue affects some unknown processing of the file /controllers/updatesettings.php. The manipulation of the argument Password leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8407	A vulnerability, which was classified as critical, has been found in code-projects Vehicle Management 1.0. This issue affects some unknown processing of the file /filter2.php. The manipulation of the argument from leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-54865	Tilesheets MediaWiki Extension adds a table lookup parser function for an item and returns the requested image. A missing backtick in a query executed by the Tilesheets extension allows users to insert and potentially execute malicious SQL code. This issue has not been fixed.	7.3	More Details
CVE-2025-8408	A vulnerability, which was classified as critical, was found in code-projects Vehicle Management 1.0. Affected is an unknown function of the file /filter1.php. The manipulation of the argument vehicle 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-2025-8409	A vulnerability has been found in code-projects Vehicle Management 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /filter.php. The manipulation of the argument from leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-54595	Pearcleaner is a free, source-available and fair-code licensed mac app cleaner. The PearcleanerHelper is a privileged helper tool bundled with the Pearcleaner application. It is registered and activated only after the user approves a system prompt to allow privileged operations. Upon approval, the helper is configured as a LaunchDaemon and runs with root privileges. In versions 4.4.0 through 4.5.1, the helper registers an XPC service (com.alienator88.Pearcleaner.PearcleanerHelper) and accepts unauthenticated connections from any local process. It exposes a method that executes arbitrary shell commands. This allows any local unprivileged user to escalate privileges to root once the helper is approved and active. This issue is fixed in version 4.5.2.	7.3	More Details
CVE-2025-8326	A vulnerability classified as critical has been found in code-projects Exam Form Submission 1.0. Affected is an unknown function of the file /admin/delete_s7.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8348	A vulnerability has been found in Kehua Charging Pile Cloud Platform 1.0 and classified as critical. This vulnerability affects unknown code of the file /home. The manipulation leads to improper authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any	7.3	More Details

	way.		
CVE-2025-8466	A vulnerability was found in code-projects Online Farm System 1.0. It has been classified as critical. Affected is an unknown function of the file /forgot_passfarmer.php. The manipulation of the argument email 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-2025-26064	A cross-site scripting (XSS) vulnerability in Intelbras RX1500 v2.2.9 and RX3000 v1.0.11 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name of a connnected device.	7.3	More Details
CVE-2025-8467	A vulnerability was found in code-projects Wazifa System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /controllers/regcontrol.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8468	A vulnerability was found in code-projects Wazifa System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /controllers/reset.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8469	A vulnerability classified as critical has been found in SourceCodester Online Hotel Reservation System 1.0. This affects an unknown part of the file /admin/deletegallery.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8470	A vulnerability classified as critical was found in SourceCodester Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /admin/deleteroom.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8441	A vulnerability, which was classified as critical, was found in code-projects Online Medicine Guide 1.0. Affected is an unknown function of the file /pharsignup.php. The manipulation of the argument phuname 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-2025-23277	NVIDIA Display Driver for Linux and Windows contains a vulnerability in the kernel mode driver, where an attacker could access memory outside bounds permitted under normal use cases. A successful exploit of this vulnerability might lead to denial of service, data tampering, or information disclosure.	7.3	More Details
CVE-2025-8471	A vulnerability, which was classified as critical, has been found in projectworlds Online Admission System 1.0. This issue affects some unknown processing of the file /adminlogin.php. The manipulation of the argument a_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-45955	Rocket Software Rocket Zena 4.4.1.26 is vulnerable to SQL Injection via the filter parameter.	7.3	More Details
CVE-2025-8378	A vulnerability was found in Campcodes Online Hotel Reservation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/index.php of the component Login. The manipulation of the argument username/password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8442	A vulnerability has been found in code-projects Online Medicine Guide 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /cussignup.php. The manipulation of the argument uname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8329	A vulnerability, which was classified as critical, was found in code-projects Vehicle Management 1.0. This affects an unknown part of the file /filter3.php. The manipulation of the argument company leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-8443	A vulnerability was found in code-projects Online Medicine Guide 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument uname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE-2025-8376	A vulnerability classified as critical has been found in code-projects Vehicle Management 1.0. Affected is an unknown function of the file /updatebal.php. The manipulation of the argument company 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-2025-8502	A vulnerability classified as critical was found in code-projects Online Medicine Guide 1.0. Affected by this vulnerability is an unknown functionality of the file /changepass.php. The manipulation of the argument ups leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8431	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/add-boat.php. The manipulation of the argument boatname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-8328	A vulnerability, which was classified as critical, has been found in code-projects Exam Form Submission 1.0. Affected by this issue is some unknown functionality of the file /register.php. The manipulation of the argument USN leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-8327	A vulnerability classified as critical was found in code-projects Exam Form Submission 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/delete_s8.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-45769	php-jwt v6.11.0 was discovered to contain weak encryption.	7.3	More Details
CVE-2025-36611	Dell Encryption and Dell Security Management Server, versions prior to 11.11.0, contain an Improper Link Resolution Before File Access ('Link Following') Vulnerability. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation.	7.3	More Details
CVE-2025-46359	A path traversal issue exists in backup and restore feature of multiple versions of PowerCMS. A product administrator may execute arbitrary code by restoring a crafted backup file.	7.2	More Details
CVE-2025-8213	The NinjaScanner – Virus & Malware scan plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'nscan_ajax_quarantine' and 'nscan_quarantine_select' functions in all versions up to, and including, 3.2.5. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, including files outside the WordPress root directory.	7.2	More Details
CVE-2025-54593	FreshRSS is a free, self-hostable RSS aggregator. In versions 1.26.1 and below, an authenticated administrator user can execute arbitrary code on the FreshRSS server by modifying the update URL to one they control, and gain code execution after running an update. After successfully executing code, user data including hashed passwords can be exfiltrated, the instance can be defaced when file permissions allow. Malicious code can be inserted into the instance to steal plaintext passwords, among others. This is fixed in version 1.26.2.	7.2	More Details
CVE-2025-5999	A privileged Vault operator with write permissions to the root namespace’s identity endpoint could escalate their own or another user’s token privileges to Vault’s root policy. Fixed in Vault Community Edition 1.20.0 and Vault Enterprise 1.20.0, 1.19.6, 1.18.11 and 1.16.22.	7.2	More Details
CVE-2025-41688	A high privileged remote attacker can execute arbitrary OS commands using an undocumented method allowing to escape the implemented LUA sandbox.	7.2	More Details
CVE-2025-54136	Cursor is a code editor built for programming with AI. In versions 1.2.4 and below, attackers can achieve remote and persistent code execution by modifying an already trusted MCP configuration file inside a shared GitHub repository or editing the file locally on the target's machine. Once a collaborator accepts a harmless MCP, the attacker can silently swap it for a malicious command (e.g., calc.exe) without triggering any warning or re-prompt. If an attacker has write permissions on a user's active branches of a source repository that contains existing MCP servers the user has previously approved, or allows an attacker has arbitrary file-write locally, the attacker can achieve arbitrary code execution. This is fixed in version 1.3.	7.2	More Details

CVE-2025-44139	Emlog Pro V2.5.7 is vulnerable to Unrestricted Upload of File with Dangerous Type via /emlog/admin/plugin.php?action=upload_zip	7.2	More Details
CVE-2025-7725	The Photos, Files, YouTube, Twitter, Instagram, TikTok, Ecommerce Contest Gallery – Upload, Vote, Sell via PayPal or Stripe, Social Share Buttons, OpenAI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the comment feature in all versions up to, and including, 26.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-49083	CVE-2025-49083 is a vulnerability in the management console of Absolute Secure Access after version 12.00 and prior to version 13.56. Attackers with administrative access to the console can cause unsafe content to be deserialized and executed in the security context of the console. The attack complexity is low and there are no attack requirements. Privileges required are high and there is no user interaction required. The impact to confidentiality is low, impact to integrity is high and there is no impact to availability. The impact to the confidentiality and integrity of subsequent systems is low and there is no subsequent system impact to availability.	7.2	More Details
CVE-2025-7050	The Use-your-Drive | Google Drive plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in file metadata in all versions up to, and including, 3.3.1 due to insufficient input sanitization and output escaping. This makes it possible for attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability can be exploited by the lowest authentication level permitted to upload files, including unauthenticated users, once a file upload shortcode is published on a publicly accessible post.	7.2	More Details
CVE-2025-38739	Dell Digital Delivery, versions prior to 5.6.1.0, contains an Insufficiently Protected Credentials vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to Information Disclosure.	7.2	More Details
CVE-2025-43224	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in visionOS 2.6, tvOS 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	7.1	More Details
CVE-2025-8312	Deadlock in PAM automatic check-in feature in Devolutions Server allows a password to remain valid beyond the end of its intended check-out period due to a deadlock occurring in the scheduling service.This issue affects the following version(s) : * Devolutions Server 2025.2.5.0 and earlier	7.1	More Details
CVE-2025-54586	GitProxy is an application that stands between developers and a Git remote endpoint. In versions 1.19.1 and below, attackers can inject extra commits into the pack sent to GitHub, commits that aren't pointed to by any branch. Although these "hidden" commits never show up in the repository's visible history, GitHub still serves them at their direct commit URLs. This lets an attacker exfiltrate sensitive data without ever leaving a trace in the branch view. We rate this a High-impact vulnerability because it completely compromises repository confidentiality. This is fixed in version 1.19.2.	7.1	More Details
CVE-2025-43239	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. Processing a maliciously crafted file may lead to unexpected app termination.	7.1	More Details
CVE-2025-43254	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. Processing a maliciously crafted file may lead to unexpected app termination.	7.1	More Details
CVE-2025-43221	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, visionOS 2.6, tvOS 18.6. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	7.1	More Details
CVE-2025-23278	NVIDIA Display Driver for Windows and Linux contains a vulnerability where an attacker might cause an improper index validation by issuing a call with crafted parameters. A successful exploit of this vulnerability might lead to data tampering or denial of service.	7.1	More Details
CVE-2025-25011	An uncontrolled search path element vulnerability can lead to local privilege Escalation (LPE) via Insecure Directory Permissions. The vulnerability arises from improper handling of directory permissions. An attacker with local access may exploit this flaw to move and delete arbitrary files, potentially gaining SYSTEM privileges.	7.0	More Details
	An uncontrolled search path element vulnerability can lead to local privilege Escalation (LPE) via		

CVE-2025-0712	Insecure Directory Permissions. The vulnerability arises from improper handling of directory permissions. An attacker with local access may exploit this flaw to move and delete arbitrary files, potentially gaining SYSTEM privileges.	7.0	More Details
CVE-2025-45770	jwt v5.4.3 was discovered to contain weak encryption.	7.0	More Details
CVE-2025-23279	NVIDIA .run Installer for Linux and Solaris contains a vulnerability where an attacker could use a race condition to escalate privileges. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, denial of service, or data tampering.	7.0	More Details
CVE-2025-23281	NVIDIA GPU Display Driver for Windows contains a vulnerability where an attacker with local unprivileged access that can win a race condition might be able to trigger a use-after-free error. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, or information disclosure.	7.0	More Details
CVE-2025-45768	pyjwt v2.10.1 was discovered to contain weak encryption.	7.0	More Details
CVE-2025-45767	jose v6.0.10 was discovered to contain weak encryption. NOTE: this is disputed by a third party because the claim of "do not meet recommended security standards" does not reflect guidance in a final publication.	7.0	More Details
CVE-2025-6037	Vault and Vault Enterprise (“Vault”) TLS certificate auth method did not correctly validate client certificates when configured with a non-CA certificate as [+trusted certificate+|https://developer.hashicorp.com/vault/api-docs/auth/cert#certificate]. In this configuration, an attacker may be able to craft a malicious certificate that could be used to impersonate another user. Fixed in Vault Community Edition 1.20.1 and Vault Enterprise 1.20.1, 1.19.7, 1.18.12, and 1.16.23.	6.8	More Details
CVE-2025-20696	In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09915215; Issue ID: MSV-3801.	6.8	More Details
CVE-2025-7694	The Woffice Core plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the woffice_file_manager_delete() function in all versions up to, and including, 5.4.26. This makes it possible for authenticated attackers, with Contributor-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).	6.8	More Details
CVE-2025-20698	In Power HAL, 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: ALPS09915400; Issue ID: MSV-3793.	6.7	More Details
CVE-2025-20697	In Power HAL, 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: ALPS09915681; Issue ID: MSV-3795.	6.7	More Details
CVE-2025-30096	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	6.7	More Details
CVE-2025-30097	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges	6.7	More Details
CVE-2025-	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements	6.7	More

30098	used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.		Details
CVE-2025-50688	A command injection vulnerability exists in TwistedWeb (version 14.0.0) due to improper input sanitization in the file upload functionality. An attacker can exploit this vulnerability by sending a specially crafted HTTP PUT request to upload a malicious file (e.g., a reverse shell script). Once uploaded, the attacker can trigger the execution of arbitrary commands on the target system, allowing for remote code execution. This could lead to escalation of privileges depending on the privileges of the web server process. The attack does not require physical access and can be conducted remotely, posing a significant risk to the confidentiality and integrity of the system.	6.5	More Details
CVE-2025-52897	GLPI is a Free Asset and IT Management Software package. In versions 9.1.0 through 10.0.18, an unauthenticated user can send a malicious link to attempt a phishing attack from the planning feature. This is fixed in version 10.0.19.	6.5	More Details
CVE-2025-43216	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 18.6, watchOS 11.6, iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9, tvOS 18.6, macOS Sequoia 15.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	6.5	More Details
CVE-2025-51060	An issue was discovered in CPUID cpuz.sys 1.0.5.4. An attacker can use DeviceIoControl with the unvalidated parameters 0x9C402440 and 0x9C402444 as IoControlCodes to perform RDMSR and WRMSR, respectively. Through this process, the attacker can modify MSR_LSTAR and hook KiSystemCall64. Afterward, using Return-Oriented Programming (ROP), the attacker can manipulate the stack with pre-prepared gadgets, disable the SMAP flag in the CR4 register, and execute a user-mode syscall handler in the kernel context. It has not been confirmed whether this works on 32-bit Windows, but it functions on 64-bit Windows if the core isolation feature is either absent or disabled.	6.5	More Details
CVE-2025-51627	Incorrect access control in CaricaVerbale in Agenzia Impresa Eccobook v2.81.1 allows authenticated attackers with low-level access to escalate privileges to Administrator.	6.5	More Details
CVE-2025-53008	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions 9.3.1 through 10.0.19, a connected user can use a malicious payload to steal mail receiver credentials. This is fixed in version 10.0.19.	6.5	More Details
CVE-2025-50867	A SQL Injection vulnerability exists in the takeassessment2.php endpoint of the CloudClassroom-PHP-Project 1.0, where the Q5 POST parameter is directly embedded in SQL statements without sanitization.	6.5	More Details
CVE-2025-54804	Russh is a Rust SSH client & server library. In versions 0.54.0 and below, the channel window adjust message of the SSH protocol is used to track the free space in the receive buffer of the other side of a channel. The current implementation takes the value from the message and adds it to an internal state value. This can result in a integer overflow. If the Rust code is compiled with overflow checks, it will panic. A malicious client can crash a server. This is fixed in version 0.54.1.	6.5	More Details
CVE-2025-50847	Cross Site Request Forgery (CSRF) vulnerability in CS Cart 4.18.3, allows attackers to add products to a user's comparison list via a crafted HTTP request.	6.5	More Details
CVE-2025-43252	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sequoia 15.6. A website may be able to access sensitive user data when resolving symlinks.	6.5	More Details
CVE-2024-34327	Sielox AnyWare v2.1.2 was discovered to contain a SQL injection vulnerability via the email address field of the password reset form.	6.5	More Details
CVE-2025-6014	Vault and Vault Enterprise’s (“Vault”) TOTP Secrets Engine code validation endpoint is susceptible to code reuse within its validity period. Fixed in Vault Community Edition 1.20.1 and Vault Enterprise 1.20.1, 1.19.7, 1.18.12, and 1.16.23.	6.5	More Details
CVE-2025-27931	An out-of-bounds read vulnerability exists in the EMF functionality of PDF-XChange Editor version 10.5.2.395. By using a specially crafted EMF file, an attacker could exploit this vulnerability to perform an out-of-bounds read, potentially leading to the disclosure of sensitive information.	6.5	More Details
CVE-			

2025-24188	A logic issue was addressed with improved checks. This issue is fixed in Safari 18.6, macOS Sequoia 15.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	6.5	More Details
CVE-2025-50868	A SQL Injection vulnerability exists in the takeassessment2.php file of CloudClassroom-PHP-Project 1.0. The Q4 POST parameter is not properly sanitized before being used in SQL queries.	6.5	More Details
CVE-2025-49832	Asterisk is an open source private branch exchange and telephony toolkit. In versions up to and including 18.26.2, between 20.00.0 and 20.15.0, 20.7-cert6, 21.00.0, 22.00.0 through 22.5.0, there is a remote DoS and possible RCE condition in \`asterisk/res/res_stir_shaken /verification.c\` that can be exploited when an attacker can set an arbitrary Identity header, or STIR/SHAKEN is enabled, with verification set in the SIP profile associated with the endpoint to be attacked. This is fixed in versions 18.26.3, 20.7-cert6, 20.15.1, 21.10.1 and 22.5.1.	6.5	More Details
CVE-2025-47152	An out-of-bounds read vulnerability exists in the EMF functionality of PDF-XChange Co. Ltd PDF-XChange Editor 10.6.0.396. By using a specially crafted EMF file, an attacker could exploit this vulnerability to perform an out-of-bounds read, potentially leading to the disclosure of sensitive information.	6.5	More Details
CVE-2025-43980	An issue was discovered on FIRSTNUM JC21A-04 devices through 2.01ME/FN. They enable the SSH service by default with the credentials of root/admin. The GUI doesn't offer a way to disable the account.	6.5	More Details
CVE-2025-50454	An Authentication Bypass vulnerability in Blue Access' Cobalt X1 thru 02.000.187 allows an unauthorized attacker to log into the application as an administrator without valid credentials.	6.5	More Details
CVE-2025-46206	An issue in Artifex mupdf 1.25.6, 1.25.5 allows a remote attacker to cause a denial of service via an infinite recursion in the \`mutool clean\` utility. When processing a crafted PDF file containing cyclic /Next references in the outline structure, the \`strip_outline()\` function enters infinite recursion	6.5	More Details
CVE-2025-36040	IBM Aspera Faspex 5.0.0 through 5.0.12.1 could allow an authenticated user to perform unauthorized actions due to client-side enforcement of sever side security mechanisms.	6.5	More Details
CVE-2025-54583	GitProxy is an application that stands between developers and a Git remote endpoint (e.g., github.com). Versions 1.19.1 and below allow users to push to remote repositories while bypassing policies and explicit approvals. Since checks and plugins are skipped, code containing secrets or unwanted changes could be pushed into a repository. This is fixed in version 1.19.2.	6.5	More Details
CVE-2025-45619	An issue in Aver PTC310UV2 firmware v.0.1.0000.59 allows a remote attacker to execute arbitrary code via the SendAction function	6.5	More Details
CVE-2025-4523	The IDonate – Blood Donation, Request And Donor Management System plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the admin_donor_profile_view() function in versions 2.0.0 to 2.1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to expose an administrator’s username, email address, and all donor fields.	6.5	More Details
CVE-2025-52237	An issue in the component /stl/actions/download?filePath of SSCMS v7.3.1 allows attackers to execute a directory traversal.	6.5	More Details
CVE-2025-52078	File upload vulnerability in Writebot AI Content Generator SaaS React Template thru 4.0.0, allowing remote attackers to gain escalated privileges via a crafted POST request to the /file-upload endpoint.	6.5	More Details
CVE-2025-45512	A lack of signature verification in the bootloader of DENX Software Engineering Das U-Boot (U-Boot) v1.1.3 allows attackers to install crafted firmware files, leading to arbitrary code execution.	6.5	More Details
CVE-2025-54752	Multiple versions of PowerCMS improperly neutralize formula elements in a CSV file. If a product user creates a malformed entry and a victim user downloads it as a CSV file and opens it in the user's environment, the embedded code may be executed.	6.5	More Details
CVE-2025-	Multiple versions of PowerCMS allow unrestricted upload of dangerous files. If a product administrator accesses a malicious file uploaded by a product user, an arbitrary script may be	6.5	More

54757	executed on the browser.		Details
CVE-2025-36039	IBM Aspera Faspex 5.0.0 through 5.0.12.1 could allow an authenticated user to perform unauthorized actions due to client-side enforcement of sever side security mechanisms,	6.5	More Details
CVE-2025-43212	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	6.5	More Details
CVE-2025-54349	In iperf before 3.19.1, iperf_auth.c has an off-by-one error and resultant heap-based buffer overflow.	6.5	More Details
CVE-2025-54585	GitProxy is an application that stands between developers and a Git remote endpoint. In versions 1.19.1 and below, attackers can exploit the way GitProxy handles new branch creation to bypass the approval of prior commits on the parent branch. The vulnerability impacts all users or organizations relying on GitProxy to enforce policy and prevent unapproved changes. It requires no elevated privileges beyond regular push access, and no extra user interaction. It does however, require a GitProxy administrator or designated user (canUserApproveRejectPush) to approve pushes to the child branch. This is fixed in version 1.19.2.	6.5	More Details
CVE-2025-53111	GLPI is a Free Asset and IT Management Software package. In versions 0.80 through 10.0.18, a lack of permission checks can result in unauthorized access to some resources. This is fixed in version 10.0.19.	6.5	More Details
CVE-2025-50464	A buffer overflow vulnerability exists in the upload.cgi module of the iptime NAS firmware v1.5.04. The vulnerability arises due to the unsafe use of the strcpy function to copy attacker-controlled data from the CONTENT_TYPE HTTP header into a fixed-size stack buffer (v8, allocated 8 bytes) without bounds checking. Since this operation occurs before authentication logic is executed, the vulnerability is exploitable pre-authentication.	6.5	More Details
CVE-2025-36608	Dell SmartFabric OS10 Software, versions prior to 10.6.0.5, contains an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	6.5	More Details
CVE-2025-30480	Dell PowerProtect Data Manager, versions prior to 19.19, contain(s) an Improper Input Validation vulnerability in PowerProtect Data Manager. A low privileged attacker with remote access could potentially exploit this vulnerability to read arbitrary files.	6.5	More Details
CVE-2024-45183	An issue was discovered in Samsung Mobile Processor Exynos 2100, 1280, 2200, 1330, 1380, 1480, and 2400. A lack of a JPEG length check leads to an out-of-bound write.	6.5	More Details
CVE-2025-25692	A PHAR deserialization vulnerability in the _getHeaders function of PrestaShop v8.2.0 allows attackers to execute arbitrary code via a crafted POST request.	6.5	More Details
CVE-2025-54656	** UNSUPPORTED WHEN ASSIGNED ** Improper Output Neutralization for Logs vulnerability in Apache Struts. This issue affects Apache Struts Extras: before 2. When using LookupDispatchAction, in some cases, Struts may print untrusted input to the logs without any filtering. Specially-crafted input may lead to log output where part of the message masquerades as a separate log line, confusing consumers of the logs (either human or automated). As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.5	More Details
CVE-2025-43214	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, watchOS 11.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, macOS Sequoia 15.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	6.5	More Details
CVE-2025-25691	A PHAR deserialization vulnerability in the component /themes/import of PrestaShop v8.2.0 allows attackers to execute arbitrary code via a crafted POST request.	6.5	More Details
CVE-2025-50420	An issue in the pdfseparate utility of freedesktop poppler v25.04.0 allows attackers to cause an infinite recursion via supplying a crafted PDF file. This can lead to a Denial of Service (DoS).	6.5	More Details

CVE-2025-43213	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	6.5	More Details
CVE-2025-6228	The Sina Extension for Elementor (Header Builder, Footer Builter, Theme Builder, Slider, Gallery, Form, Modal, Data Table Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the \`Sina Posts\`, \`Sina Blog Post\` and \`Sina Table\` widgets in all versions up to, and including, 3.7.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8399	The Mmm Unity Loader plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘attributes’ parameter in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2025-33118	IBM QRadar SIEM 7.5 through 7.5.0 Update Pack 12 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.4	More Details
CVE-2025-7646	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom script parameter in all versions up to, and including, 6.3.10 even when the user does not have the unfiltered_html capability. 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-2025-52133	The Mocca Calendar application before 2.15 for XWiki allows XSS via a title upon calendar import.	6.4	More Details
CVE-2025-52132	The Mocca Calendar application before 2.15 for XWiki allows XSS via a title to the view event page.	6.4	More Details
CVE-2025-52131	The Mocca Calendar application before 2.15 for XWiki allows XSS via the background or text color field.	6.4	More Details
CVE-2025-54962	/edit-user in webserver in OpenPLC Runtime 3 through 9cd8f1b allows authenticated users to upload arbitrary files (such as .html or .svg), and these are then publicly accessible under the /static URI.	6.4	More Details
CVE-2025-8391	The Magic Edge – Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘height’ parameter in all versions up to, and including, 1.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8294	The Download Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘name’ parameter in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8295	The Employee Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘noaccess_msg’ parameter in all versions up to, and including, 4.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8317	The Custom Word Cloud plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘angle’ parameter in all versions up to, and including, 0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an	6.4	More Details

	injected page.		
CVE-2025-7845	The Stratum – Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Advanced Google Maps and Image Hotspot widgets in all versions up to, and including, 1.6.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8212	The Medical Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Typewriter widget in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-4684	The BlockSpare: Gutenberg Blocks & Patterns for Blogs, Magazines, Business Sites – Post Grids, Sliders, Carousels, Counters, Page Builder & Starter Site Imports, No Coding Needed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTML attributes of Image Carousel and Image Slider widgets in all versions up to, and including, 3.2.13.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-4588	The 360 Photo Spheres plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sphere' shortcode in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8146	The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's TypeOut Text widget in all versions up to, and including, 1.9.2 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-2025-8315	The WP Easy Contact plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘noaccess_msg’ parameter in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-54131	Cursor is a code editor built for programming with AI. In versions below 1.3, an attacker can bypass the allow list in auto-run mode with a backtick (`) or $(cmd). If a user has swapped Cursor from its default settings (requiring approval for every terminal call) to an allowlist, an attacker can execute arbitrary command execution outside of the allowlist without user approval. An attacker can trigger this vulnerability if chained with indirect prompt injection. This is fixed in version 1.3.	6.4	More Details
CVE-2025-5720	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘author’ parameter in all versions up to, and including, 5.80.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8313	The Campus Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘noaccess_msg’ parameter in all versions up to, and including, 1.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7500	The Ocean Social Sharing plugin for WordPress is vulnerable to Stored Cross-Site Scripting via social icon titles in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8347	A vulnerability, which was classified as critical, was found in Kehua Charging Pile Cloud Platform 1.0. This affects an unknown part of the file /sys/task/findAllTask. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE-2025-8382	A vulnerability, which was classified as critical, was found in Campcodes Online Hotel Reservation System 1.0. Affected is an unknown function of the file /admin/edit_room.php. The manipulation of the argument room_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8517	A vulnerability was found in givanz Vvveb 1.0.6.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to session fixiation. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.7 is able to address this issue. The patch is named d4b1e030066417b77d15b4ac505eed5ae7bf2c5e. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-8345	A vulnerability classified as critical was found in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.4.7. Affected by this vulnerability is the function delete_user of the file crm/WeiXinApp/yunzhijia/yunzhijiaApi.php. The manipulation of the argument function leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 8.6.5.2 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2025-8500	A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /insert-and-view/action.php. The manipulation of the argument content leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8504	A vulnerability, which was classified as critical, was found in code-projects Kitchen Treasure 1.0. This affects an unknown part of the file /userregistration.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8344	A vulnerability classified as critical has been found in openviglet shio up to 0.3.8. Affected is the function shStaticFileUpload of the file shio-app/src/main/java/com/viglet/shio/api/staticfile/ShStaticFileAPI.java. The manipulation of the argument filename leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8381	A vulnerability, which was classified as critical, has been found in Campcodes Online Hotel Reservation System 1.0. This issue affects some unknown processing of the file /add_reserve.php. The manipulation of the argument room_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-54589	Copyparty is a portable file server. In versions 1.18.6 and below, when accessing the recent uploads page at `/?ru`, users can filter the results using an input field at the top. This field appends a filter parameter to the URL, which reflects its value directly into a `<script>` block without proper escaping, allowing for reflected Cross-Site Scripting (XSS) and can be exploited against both authenticated and unauthenticated users. This is fixed in version 1.18.7.	6.3	More Details
CVE-2024-34328	An open redirect in Sielox AnyWare v2.1.2 allows attackers to execute a man-in-the-middle attack via a crafted URL.	6.3	More Details
CVE-2025-8526	A vulnerability was found in Exrick xboot up to 3.3.4. It has been declared as critical. This vulnerability affects the function Upload of the file xboot-fast/src/main/java/cn/exrick/xboot/modules/base/controller/common/UploadController.java. The manipulation of the argument File leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8527	A vulnerability was found in Exrick xboot up to 3.3.4. It has been rated as critical. This issue affects some unknown processing of the file xboot-fast/src/main/java/cn/exrick/xboot/modules/base/controller/common/SecurityController.java of the component Swagger. The manipulation of the argument loginUrl leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8529	A vulnerability classified as critical was found in cloudfavorites favorites-web up to 1.3.0. Affected by this vulnerability is the function getCollectLogoUrl of the file app/src/main/java/com/favorites/web/CollectController.java. The manipulation of the argument url leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE-2025-43211	The issue was addressed with improved memory handling. This issue is fixed in Safari 18.6, macOS Sequoia 15.6, iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6, tvOS 18.6, watchOS 11.6, visionOS 2.6. Processing web content may lead to a denial-of-service.	6.2	More Details
CVE-2025-43191	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to cause a denial-of-service.	6.2	More Details
CVE-2025-43240	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, Safari 18. 6. A download's origin may be incorrectly associated.	6.2	More Details
CVE-2025-31275	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6. A sandboxed process may be able to launch any installed app.	6.2	More Details
CVE-2025-8400	The Image Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2025-6832	The All in One Time Clock Lite – Tracking Employee Time Has Never Been Easier plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'nonce' parameter in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-51502	Reflected Cross-Site Scripting (XSS) in Microweber CMS 2.0 via the layout parameter on the /admin/page/create page allows arbitrary JavaScript execution in the context of authenticated admin users.	6.1	More Details
CVE-2025-36605	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'). An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	6.1	More Details
CVE-2025-51857	The reconcile method in the AttachmentReconciler class of the Halo system v.2.20.18LTS and before is vulnerable to XSS attacks.	6.1	More Details
CVE-2024-41177	Incomplete Blacklist to Cross-Site Scripting vulnerability in Apache Zeppelin. This issue affects Apache Zeppelin: before 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue.	6.1	More Details
CVE-2025-45778	A stored cross-site scripting (XSS) vulnerability in The Language Sloth Web Application v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Description text field.	6.1	More Details
CVE-2024-52890	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.03 could be susceptible to cross-site scripting due to no validation of URIs.	6.1	More Details
CVE-2025-50869	A stored Cross-Site Scripting (XSS) vulnerability exists in the qureydetails.php page of Institute-of-Current-Students 1.0, where the input fields for Query and Answer do not properly sanitize user input. Authenticated users can inject arbitrary JavaScript code.	6.1	More Details
CVE-2025-51501	Reflected Cross-Site Scripting (XSS) in the id parameter of the live_edit.module_settings API endpoint in Microweber CMS2.0 allows execution of arbitrary JavaScript.	6.1	More Details
CVE-2024-45515	An issue was discovered in Zimbra Collaboration (ZCS) through 10.1. A Cross-Site Scripting (XSS) vulnerability exists in Zimbra webmail due to insufficient validation of the content type metadata when importing files into the briefcase. Attackers can exploit this issue by crafting a file with manipulated metadata, allowing them to bypass content type checks and execute arbitrary JavaScript within the victim's session.	6.1	More Details

CVE-2025-43229	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.6, Safari 18. 6. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2025-51951	andisearch v0.5.249 was discovered to contain a cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2025-51954	playground.electronhub.ai v1.1.9 was discovered to contain a cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2025-8319	the BMA login interface allows arbitrary JavaScript or HTML to be written straight into the page’s Document Object Model via the error= URL parameter	6.1	More Details
CVE-2025-50848	A file upload vulnerability was discovered in CS Cart 4.18.3, allows attackers to execute arbitrary code. CS Cart 4.18.3 allows unrestricted upload of HTML files, which are rendered directly in the browser when accessed. This allows an attacker to upload a crafted HTML file containing malicious content, such as a fake login form for credential harvesting or scripts for Cross-Site Scripting (XSS) attacks. Since the content is served from a trusted domain, it significantly increases the likelihood of successful phishing or script execution against other users.	6.1	More Details
CVE-2025-51569	A cross-site scripting (XSS) vulnerability exists in the LB-Link BL-CPE300M 01.01.02P42U14_06 router's web interface. The /goform/goform_get_cmd_process endpoint fails to sanitize user input in the cmd parameter before reflecting it into a text/html response. This allows unauthenticated attackers to inject arbitrary JavaScript, which is executed in the context of the router's origin when the crafted URL is accessed. The issue requires user interaction to exploit.	6.1	More Details
CVE-2025-36563	Reflected cross-site scripting vulnerability exists in multiple versions of PowerCMS. If a product administrator accesses a crafted URL, an arbitrary script may be executed on the browser.	6.1	More Details
CVE-2025-50270	A stored Cross Site Scripting (xss) vulnerability in the "content management" feature in AnQiCMS v.3.4.11 allows a remote attacker to execute arbitrary code via a crafted script to the title, categoryTitle, and tmpTag parameters.	6.1	More Details
CVE-2025-50866	CloudClassroom-PHP-Project 1.0 contains a reflected Cross-site Scripting (XSS) vulnerability in the email parameter of the postquerypublic endpoint. Improper sanitization allows an attacker to inject arbitrary JavaScript code that executes in the context of the user s browser, potentially leading to session hijacking or phishing attacks.	6.1	More Details
CVE-2025-24854	A carefully crafted request using the Image plugin could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.12.3 or later.	6.1	More Details
CVE-2025-4426	The vulnerability was identified in the code developed specifically for Lenovo. Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the vulnerability. https://support.lenovo.com/us/en/product_security/home	6.0	More Details
CVE-2025-37112	A vulnerability was discovered in the storage policy for certain sets of encryption keys in the HPE Telco Network Function Virtual Orchestrator. Successful Exploitation could lead to unauthorized parties gaining access to sensitive system information.	6.0	More Details
CVE-2025-37111	A vulnerability was discovered in the storage policy for certain sets of authentication keys in the HPE Telco Network Function Virtual Orchestrator. Successful Exploitation could lead to unauthorized parties gaining access to sensitive system information.	6.0	More Details
CVE-2025-37110	A vulnerability was discovered in the storage policy for certain sets of sensitive credential information in the HPE Telco Network Function Virtual Orchestrator. Successful Exploitation could lead to unauthorized parties gaining access to sensitive system information.	6.0	More Details
CVE-2025-4424	The vulnerability was identified in the code developed specifically for Lenovo. Please visit "Lenovo Product Security Advisories and Announcements" webpage for more information about the vulnerability. https://support.lenovo.com/us/en/product_security/home	6.0	More Details
CVE-2023-32253	A flaw was found in the Linux kernel's ksmbd component. A deadlock is triggered by sending multiple concurrent session setup requests, possibly leading to a denial of service.	5.9	More Details

CVE-2025-8353	UI synchronization issue in the Just-in-Time (JIT) access request approval interface in Devolutions Server 2025.2.4.0 and earlier allows a remote authenticated attacker to gain unauthorized access to deleted JIT Groups via stale UI state during standard checkout request processing.	5.9	More Details
CVE-2023-2593	A flaw exists within the Linux kernel's handling of new TCP connections. The issue results from the lack of memory release after its effective lifetime. This vulnerability allows an unauthenticated attacker to create a denial of service condition on the system.	5.9	More Details
CVE-2025-5921	The SureForms WordPress plugin before 1.7.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against both authenticated and unauthenticated users.	5.8	More Details
CVE-2019-19145	Quantum SuperLoader 3 V94.0 005E.0h devices allow attackers to access the hardcoded fa account because there are only 65536 possible passwords.	5.8	More Details
CVE-2025-54584	GitProxy is an application that stands between developers and a Git remote endpoint (e.g., github.com). In versions 1.19.1 and below, an attacker can craft a malicious Git packfile to exploit the PACK signature detection in the parsePush.ts file. By embedding a misleading PACK signature within commit content and carefully constructing the packet structure, the attacker can trick the parser into treating invalid or unintended data as the packfile. Potentially, this would allow bypassing approval or hiding commits. This issue is fixed in version 1.19.2.	5.7	More Details
CVE-2025-6015	Vault and Vault Enterprise’s (“Vault”) login MFA rate limits could be bypassed and TOTP tokens could be reused. Fixed in Vault Community Edition 1.20.1 and Vault Enterprise 1.20.1, 1.19.7, 1.18.12, and 1.16.23.	5.7	More Details
CVE-2025-46809	A Insertion of Sensitive Information into Log File vulnerability in SUSE Multi Linux Manager exposes the HTTP proxy credentials. This issue affects Container suse/manager/5.0/x86_64/server:5.0.5.7.30.1: from ? before 5.0.27-150600.3.33.1; Image SLES15-SP4-Manager-Server-4-3-BYOS: from ? before 4.3.87-150400.3.110.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-Azure: from ? before 4.3.87-150400.3.110.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-EC2: from ? before 4.3.87-150400.3.110.2; Image SLES15-SP4-Manager-Server-4-3-BYOS-GCE: from ? before 4.3.87-150400.3.110.2; SUSE Manager Server Module 4.3: from ? before 4.3.87-150400.3.110.2.	5.7	More Details
CVE-2025-23289	NVIDIA Omniverse Launcher for Windows and Linux contains a vulnerability in the launcher logs, where a user could cause sensitive information to be written to the log files through proxy servers. A successful exploit of this vulnerability might lead to information disclosure.	5.5	More Details
CVE-2025-23285	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where it allows a guest to access global resources. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2025-54871	Electron Capture facilitates video playback for screen-sharing and capture. In versions 2.19.1 and below, the elecap app on macOS allows local unprivileged users to bypass macOS TCC privacy protections by enabling ELECTRON_RUN_AS_NODE. This environment variable allows arbitrary Node.js code to be executed via the -e flag, which runs inside the main Electron context, inheriting any previously granted TCC entitlements (such as access to Documents, Downloads, etc.). This issue is fixed in version 2.20.0.	5.5	More Details
CVE-2025-30103	Dell SmartFabric OS10 Software, versions prior to 10.6.0.5 contains a Files or Directories Accessible to External Parties vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	5.5	More Details
CVE-2025-50422	An issue was discovered in freedesktop poppler v25.04.0. The heap memory containing PDF stream objects is not cleared upon program exit, allowing attackers to obtain sensitive PDF content via a memory dump.	5.5	More Details
CVE-2025-43185	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sequoia 15.6. An app may be able to access protected user data.	5.5	More Details
CVE-2025-43218	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted USD file may disclose memory contents.	5.5	More Details
CVE-	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia		More

2025-43225	15.6, iPadOS 17.7.9, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to access sensitive user data.	5.5	Details
CVE-2025-43247	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. A malicious app with root privileges may be able to modify the contents of system files.	5.5	More Details
CVE-2025-43215	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2025-43235	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.6. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2025-43241	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to read files outside of its sandbox.	5.5	More Details
CVE-2025-43267	An injection issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43246	This issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43251	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.6. A local attacker may gain access to Keychain items.	5.5	More Details
CVE-2025-43195	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-2810	A low privileged local attacker can abuse the affected service by using a hardcoded cryptographic key.	5.5	More Details
CVE-2025-41658	CODESYS Runtime Toolkit-based products may expose sensitive files to local low-privileged operating system users due to default file permissions.	5.5	More Details
CVE-2025-29557	ExaGrid EX10 6.3 - 7.0.1.P08 is vulnerable to Incorrect Access Control in the MailConfiguration API endpoint, where users with operator-level privileges can issue an HTTP request to retrieve SMTP credentials, including plaintext passwords.	5.4	More Details
CVE-2025-41391	Stored cross-site scripting vulnerability exists in multiple versions of PowerCMS. If a product user accesses a malicious page, an arbitrary script may be executed on the browser.	5.4	More Details
CVE-2025-6078	Partner Software's Partner Software application and Partner Web application allows an authenticated user to add notes on the 'Notes' page when viewing a job but does not completely sanitize input, making it possible to add notes with HTML tags and JavaScript, enabling an attacker to add a note containing malicious JavaScript, leading to stored XSS (cross-site scripting).	5.4	More Details
CVE-2025-41396	A path traversal issue exists in file uploading feature of multiple versions of PowerCMS. Arbitrary files may be overwritten by a product user.	5.4	More Details
CVE-2025-53357	GLPI, which stands for Gestionnaire Libre de Parc Informatique, is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions 0.78 through 10.0.18, a connected user can alter the reservations of another user. This is fixed in version 10.0.19.	5.4	More Details
CVE-2025-	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the donor notes parameter in all versions up to, and including, 4.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with GiveWP worker-level access and above, to inject arbitrary web scripts in pages that	5.4	More Details

7205	will execute whenever a user accesses an injected page. Additionally, they need to trick an administrator into visiting the legacy version of the site.		
CVE-2025-8433	A vulnerability was found in code-projects Document Management System 1.0 and classified as critical. This issue affects the function unlink of the file /dell.php. The manipulation of the argument ID leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	5.4	More Details
CVE-2025-46958	Adobe Experience Manager versions 6.5.22 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.	5.4	More Details
CVE-2025-47001	Adobe Experience Manager versions 6.5.22 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.	5.4	More Details
CVE-2025-50592	Cross site scripting vulnerability in seacms before 13.2 via the vid parameter to Upload/js/player/dmplayer/player.	5.4	More Details
CVE-2025-46018	CSC Pay Mobile App 2.19.4 (fixed in version 2.20.0) contains a vulnerability allowing users to bypass payment authorization by disabling Bluetooth at a specific point during a transaction. This could result in unauthorized use of laundry services and potential financial loss.	5.4	More Details
CVE-2025-54834	OPEXUS FOIAXpress Public Access Link (PAL) version v11.1.0 allows an unauthenticated, remote attacker to query the /App/CreateRequest.aspx endpoint to check for the existence of valid usernames. There are no rate-limiting mechanisms in place.	5.3	More Details
CVE-2025-54939	LiteSpeed QUIC (LSQUIC) Library before 4.3.1 has an lsquic_engine_packet_in memory leak.	5.3	More Details
CVE-2025-43276	A logic error was addressed with improved error handling. This issue is fixed in macOS Sequoia 15.6. iCloud Private Relay may not activate when more than one user is logged in at the same time.	5.3	More Details
CVE-2025-8546	A vulnerability, which was classified as problematic, was found in atjiu pybbs up to 6.0.0. This affects the function adminlogin/login of the component Verification Code Handler. The manipulation leads to guessable captcha. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The patch is named ecaf8d46944fd03e3c4ea05698f8acf0aaa570cf. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-8547	A vulnerability has been found in atjiu pybbs up to 6.0.0 and classified as critical. This vulnerability affects unknown code of the component Email Verification Handler. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 044f22893bee254dc2bb0d30f614913fab3c22c2. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-48499	Out-of-bounds write vulnerability exists in FUJIFILM Business Innovation MFPs. A specially crafted IPP (Internet Printing Protocol) or LPD (Line Printer Daemon) packet may cause a denial-of-service (DoS) condition on an affected MFP. Resetting the MFP is required to recover from the denial-of-service (DoS) condition.	5.3	More Details
CVE-2025-8513	A vulnerability, which was classified as problematic, was found in Caixin News App 8.0.1 on Android. Affected is an unknown function of the file AndroidManifest.xml of the component com.caixin.news. The manipulation leads to improper export of android application components. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-8512	A vulnerability, which was classified as problematic, has been found in TVB Big Big Shop App 2.9.0 on Android. This issue affects some unknown processing of the file AndroidManifest.xml of the component hk.com.tvb.bigbigshop. The manipulation leads to improper export of android application components. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details

CVE-2025-8530	A vulnerability, which was classified as problematic, has been found in elunez eladmin up to 2.7. Affected by this issue is some unknown functionality of the file eladmin-system\src\main\resources\config\application-prod.yml of the component Druid. The manipulation of the argument login-username/login-password leads to use of default credentials. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-51775	Missing Origin Validation in WebSockets vulnerability in Apache Zeppelin. The attacker could access the Zeppelin server from another origin without any restriction, and get internal information about paragraphs. This issue affects Apache Zeppelin: from 0.11.1 before 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue.	5.3	More Details
CVE-2024-52279	Improper Input Validation vulnerability in Apache Zeppelin. The fix for JDBC URL validation in CVE-2024-31864 did not account for URL encoded input. This issue affects Apache Zeppelin: from 0.11.1 before 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue.	5.3	More Details
CVE-2025-31276	This issue was addressed through improved state management. This issue is fixed in iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9. Remote content may be loaded even when the 'Load Remote Images' setting is turned off.	5.3	More Details
CVE-2025-6722	The BitFire Security – Firewall, WAF, Bot/Spam Blocker, Login Security plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.5 via the bitfire_* directory that automatically gets created and stores potentially sensitive files without any access restrictions. This makes it possible for unauthenticated attackers to extract sensitive data from various files like config.ini, debug.log, and more when directory listing is enabled on the server.	5.3	More Details
CVE-2025-8152	The WP CTA – Call To Action Plugin, Sticky CTA, Sticky Buttons plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_cta_status' and 'change_sticky_sidebar_name' functions in all versions up to, and including, 1.7.0. This makes it possible for unauthenticated attackers to update the status of a sticky and update the name displayed in the back-end WP CTA Dashboard.	5.3	More Details
CVE-2025-8585	A vulnerability, which was classified as critical, has been found in libav up to 12.3. Affected by this issue is the function main of the file /avtools/avconv.c of the component DSS File Demuxer. The manipulation leads to double free. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The bug was initially reported by the researcher to the wrong project. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2025-54575	ImageSharp is a 2D graphics library. In versions below 2.1.11 and 3.0.0 through 3.1.10, a specially crafted GIF file containing a malformed comment extension block (with a missing block terminator) can cause the ImageSharp GIF decoder to enter an infinite loop while attempting to skip the block. This leads to a denial of service. Applications processing untrusted GIF input should upgrade to a patched version. This issue is fixed in versions 2.1.11 and 3.1.11.	5.3	More Details
CVE-2025-8523	A vulnerability has been found in RiderLike Fruit Crush-Brain App 1.0 on Android and classified as problematic. Affected by this vulnerability is an unknown functionality of the file AndroidManifest.xml of the component com.fruitcrush.fun. The manipulation leads to improper export of android application components. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-54554	tiaudit in Tera Insights tiCrypt before 2025-07-17 allows unauthenticated REST API requests that reveal sensitive information about the underlying SQL queries and database structure.	5.3	More Details
CVE-2025-8516	A vulnerability was found in Kingdee Cloud-Starry-Sky Enterprise Edition up to 8.2. It has been classified as problematic. Affected is the function BaseServiceFactory.getFileUploadService.deleteFileAction of the file K3Cloud\BBCMallSite\WEB-INF\lib\Kingdee.K3.O2O.Base.WebApp.jar!\kingdee\k3\o2o\base\webapp\action\FileUploadAction.class of the component IIS-K3CloudMiniApp. The manipulation of the argument filePath leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor recommends as a short-term measure to "[t]emporarily disable external network access to the Kingdee Cloud Galaxy Retail System or set up an IP whitelist for access control." The long-term remediation will be: "Install the security patch provided by the Starry Sky system, with the specific solutions being: i) Adding authentication to the vulnerable CMKAppWebHandler.ashx interface; ii) Removing the file reading function."	5.3	More Details
CVE-2025-	Vault and Vault Enterprise’s (“Vault”) user lockout feature could be bypassed for Userpass and LDAP authentication methods. Fixed in Vault Community Edition 1.20.1 and Vault Enterprise 1.20.1,	5.3	More

6004	1.19.7, 1.18.12, and 1.16.23.		Details
CVE-2025-8524	A vulnerability was found in Boquan DotWallet App 2.15.2 on Android and classified as problematic. Affected by this issue is some unknown functionality of the file AndroidManifest.xml of the component com.boquanhash.dotwallet. The manipulation leads to improper export of android application components. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-54425	Umbraco is an ASP.NET CMS. In versions 13.0.0 through 13.9.2, 15.0.0 through 15.4.1 and 16.0.0 through 16.1.0, the content delivery API can be restricted from public access where an API key must be provided in a header to authorize the request. It's also possible to configure output caching, such that the delivery API outputs will be cached for a period of time, improving performance. There's an issue when these two things are used together, where caching doesn't vary by the header that contains the API key. As such, it's possible for a user without a valid API key to retrieve a response for a given path and query if it has recently been requested and cached by request with a valid key. This is fixed in versions 13.9.3, 15.4.4 and 16.1.1.	5.3	More Details
CVE-2025-8525	A vulnerability was found in Exrick xboot up to 3.3.4. It has been classified as problematic. This affects an unknown part of the component Spring Boot Admin/Spring Actuator. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2025-44958	RUCKUS Network Director (RND) before 4.5 stores passwords in a recoverable format.	5.3	More Details
CVE-2023-32255	A flaw was found in the Linux kernel's ksmbd component. A memory leak can occur if a client sends a session setup request with an unknown NTLMSSP message type, potentially leading to resource exhaustion.	5.3	More Details
CVE-2025-5988	A flaw was found in the Ansible aap-gateway. Cross-site request forgery (CSRF) origin checking is not done on requests from the gateway to external components, such as the controller, hub, and eda.	5.3	More Details
CVE-2025-54833	OPEXUS FOIAXpress Public Access Link (PAL) version v11.1.0 allows attackers to bypass account-lockout and CAPTCHA protections. Unauthenticated remote attackers can more easily brute force passwords.	5.3	More Details
CVE-2025-31716	In bootloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed.	5.1	More Details
CVE-2025-43260	This issue was addressed with improved data protection. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7. An app may be able to hijack entitlements granted to other privileged apps.	5.1	More Details
CVE-2025-43266	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	5.1	More Details
CVE-2025-8341	Grafana is an open-source platform for monitoring and observability. The Infinity datasource plugin, maintained by Grafana Labs, allows visualizing data from JSON, CSV, XML, GraphQL, and HTML endpoints. If the plugin was configured to allow only certain URLs, an attacker could bypass this restriction using a specially crafted URL. This vulnerability is fixed in version 3.4.1.	5.0	More Details
CVE-2025-8522	A vulnerability, which was classified as critical, was found in givanz Vvvebjs up to 2.0.4. Affected is an unknown function of the file /save.php of the component node.js. The manipulation of the argument File leads to path traversal. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used.	5.0	More Details
CVE-2025-44962	RUCKUS SmartZone (SZ) before 6.1.2p3 Refresh Build allows ../ directory traversal to read files.	5.0	More Details
	The Smart Slider 3 plugin for WordPress is vulnerable to time-based SQL Injection via the ‘sliderid’		

CVE-2025-6348	parameter in all versions up to, and including, 3.5.1.28 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-2025-8518	A vulnerability was found in givanz Vvveb 1.0.5. It has been rated as critical. Affected by this issue is the function Save of the file admin/controller/editor/code.php of the component Code Editor. The manipulation leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.6 is able to address this issue. The name of the patch is f684f3e374d04db715730fc4796e102f5ebcacb2. It is recommended to upgrade the affected component.	4.7	More Details
CVE-2025-8520	A vulnerability classified as critical was found in givanz Vvveb up to 1.0.5. This vulnerability affects unknown code of the file /vadmin123/?module=editor/editor of the component Drag-and-Drop Editor. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.6 is able to address this issue. The patch is identified as f684f3e374d04db715730fc4796e102f5ebcacb2. It is recommended to upgrade the affected component.	4.7	More Details
CVE-2025-55014	The YouDao plugin for StarDict, as used in stardict 3.0.7+git20220909+dfsg-6 in Debian trixie and elsewhere, sends an X11 selection to the dict.youdao.com and dict.cn servers via cleartext HTTP.	4.7	More Details
CVE-2025-8379	A vulnerability classified as critical has been found in Campcodes Online Hotel Reservation System 1.0. This affects an unknown part of the file /admin/edit_room.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-43259	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2025-52892	EspoCRM is a web application with a frontend designed as a single-page application and a REST API backend written in PHP. In versions 9.1.6 and below, if a user loads Espo in the browser with double slashes (e.g https://domain//#Admin) and the webserver does not strip the double slash, it can cause a corrupted Slim router's cache. This will make the instance unusable until there is a completed rebuild. This is fixed in version 9.1.7.	4.5	More Details
CVE-2025-7738	A flaw was found in Ansible Automation Platform (AAP) where the Gateway API returns the client secret for certain GitHub Enterprise authenticators in clear text. This vulnerability affects administrators or auditors accessing authenticator configurations. While access is limited to privileged users, the clear text exposure of sensitive credentials increases the risk of accidental leaks or misuse.	4.4	More Details
CVE-2025-54132	Cursor is a code editor built for programming with AI. In versions below 1.3, Mermaid (which is used to render diagrams) allows embedding images which then get rendered by Cursor in the chat box. An attacker can use this to exfiltrate sensitive information to a third-party attacker controlled server through an image fetch after successfully performing a prompt injection. A malicious model (or hallucination/backdoor) might also trigger this exploit at will. This issue requires prompt injection from malicious data (web, image upload, source code) in order to exploit. In that case, it can send sensitive information to an attacker-controlled external server. This is fixed in version 1.3.	4.4	More Details
CVE-2025-6626	The ShortPixel Adaptive Images – WebP, AVIF, CDN, Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the API URL Setting in all versions up to, and including, 3.10.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-23286	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where an attacker could read invalid memory. A successful exploit of this vulnerability might lead to information disclosure.	4.4	More Details
CVE-2025-43274	A privacy issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.6. A sandboxed process may be able to circumvent sandbox restrictions.	4.4	More Details

CVE-2025-8068	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to unauthorized modification and loss of data due to an improper capability check on the 'ajax_trash_templates' function in all versions up to, and including, 2.9.1. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary attachment files, and move arbitrary posts, pages, and templates to the Trash.	4.3	More Details
CVE-2025-8151	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 2.9.1 via the 'save_block_css' function. This makes it possible for authenticated attackers, with Author-level access and above, to create CSS files in any directory, and delete CSS files in any directory in a Windows environment.	4.3	More Details
CVE-2025-43228	The issue was addressed with improved UI. This issue is fixed in iOS 18.6 and iPadOS 18.6, Safari 18.6. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2025-8343	A vulnerability was found in openviglet shio up to 0.3.8. It has been rated as critical. This issue affects the function shStaticFilePreUpload of the file shio-app/src/main/java/com/viglet/shio/api/staticfile/ShStaticFileAPI.java. The manipulation of the argument fileName leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-8370	A vulnerability, which was classified as problematic, was found in Portabilis i-Educar 2.9. Affected is an unknown function of the file /intranet/educar_escolaridade_lst.php. The manipulation of the argument descricao leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-8369	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.9. This issue affects some unknown processing of the file /intranet/educar_avaliacao_desempenho_lst.php. The manipulation of the argument titulo_avaliacao leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-8368	A vulnerability classified as problematic was found in Portabilis i-Educar 2.9. This vulnerability affects unknown code of the file /intranet/pesquisa_pessoa_lst.php. The manipulation of the argument campo_busca/cpf leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-8367	A vulnerability classified as problematic has been found in Portabilis i-Educar 2.9. This affects an unknown part of the file /intranet/funcionario_vinculo_lst.php. The manipulation of the argument nome leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-8366	A vulnerability was found in Portabilis i-Educar 2.9. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /intranet/educar_servidor_lst.php. The manipulation of the argument nome/matricula_servidor leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-8346	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.10. Affected by this issue is some unknown functionality of the file /educar_aluno_lst.php. The manipulation of the argument ref_cod_matricula with the input "><img%20src=x%20onerror=alert(%27CVE-Hunters%27)> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-8505	A vulnerability has been found in 495300897 wx-shop up to de1b66331368695779cfc6e4d11a64caddf8716e and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	4.3	More Details
CVE-	Use After Free vulnerability in Arm Ltd Bifrost GPU Userspace Driver, Arm Ltd Valhall GPU Userspace Driver, Arm Ltd Arm 5th Gen GPU Architecture Userspace Driver allows a non-privileged user process to perform valid GPU processing operations, including via WebGL or WebGPU, to gain access to		

2025-0932	already freed memory.This issue affects Bifrost GPU Userspace Driver: from r48p0 through r49p3, from r50p0 through r51p0; Valhall GPU Userspace Driver: from r48p0 through r49p3, from r50p0 through r54p0; Arm 5th Gen GPU Architecture Userspace Driver: from r48p0 through r49p3, from r50p0 through r54p0.	4.3	More Details
CVE-2025-8335	A vulnerability classified as problematic has been found in code-projects Simple Car Rental System 1.0. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-54573	CVAT is an open source interactive video and image annotation tool for computer vision. In versions 1.1.0 through 2.41.0, email verification was not enforced when using Basic HTTP Authentication. As a result, users could create accounts using fake email addresses and use the product as verified users. Additionally, the missing email verification check leaves the system open to bot signups and further usage. CVAT 2.42.0 and later versions contain a fix for the issue. CVAT Enterprise customers have a workaround available; those customers may disable registration to prevent this issue.	4.3	More Details
CVE-2025-53112	GLPI is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions 9.1.0 through 10.0.18, a lack of permission checks can result in unauthorized removal of some specific resources. This is fixed in version 10.0.19.	4.3	More Details
CVE-2025-50340	An Insecure Direct Object Reference (IDOR) vulnerability was discovered in SOGo Webmail thru 5.6.0, allowing an authenticated user to send emails on behalf of other users by manipulating a user-controlled identifier in the email-sending request. The server fails to verify whether the authenticated user is authorized to use the specified sender identity, resulting in unauthorized message delivery as another user. This can lead to impersonation, phishing, or unauthorized communication within the system.	4.3	More Details
CVE-2025-8401	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.9.1 via the 'get_post_data' function. This makes it possible for authenticated attackers, with Author-level access and above, to extract sensitive data including the content of private, password-protected, and draft posts and pages.	4.3	More Details
CVE-2025-8340	A vulnerability was found in code-projects Intern Membership Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file fill_details.php of the component Error Message Handler. The manipulation of the argument email leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-8488	The Ultimate Addons for Elementor (Formerly Elementor Header & Footer Builder) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_hfe_compatibility_option_callback ()function in all versions up to, and including, 2.4.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the compatibility option setting.	4.3	More Details
CVE-2025-54832	OPEXUS FOIAXpress Public Access Link (PAL), version v11.1.0, allows an authenticated user to add entries to the list of states and territories.	4.3	More Details
CVE-2025-43230	The issue was addressed with additional permissions checks. This issue is fixed in iPadOS 17.7.9, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. An app may be able to access user-sensitive data.	4.0	More Details
CVE-2025-8217	The Amazon Q Developer Visual Studio Code (VS Code) extension v1.84.0 contains inert, injected code designed to call the Q Developer CLI. The code executes when the extension is launched within the VS Code environment; however the injected code contains a syntax error which prevents it from making a successful API call to the Q Developer CLI. To mitigate this issue, users should upgrade to version v1.85.0. All installations of v1.84.0 should be removed from use.	4.0	More Details
CVE-2025-43265	An out-of-bounds read was addressed with improved input validation. This issue is fixed in Safari 18.6, watchOS 11.6, visionOS 2.6, iOS 18.6 and iPadOS 18.6, macOS Sequoia 15.6, tvOS 18.6. Processing maliciously crafted web content may disclose internal states of the app.	4.0	More Details
CVE-2025-43250	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to break out of its sandbox.	4.0	More Details
	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS		

CVE-2025-43226	11.6, iOS 18.6 and iPadOS 18.6, iPadOS 17.7.9, tvOS 18.6, macOS Sequoia 15.6, macOS Sonoma 14.7.7, visionOS 2.6. Processing a maliciously crafted image may result in disclosure of process memory.	4.0	More Details
CVE-2025-43217	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.9, iOS 18.6 and iPadOS 18.6. Privacy Indicators for microphone or camera access may not be correctly displayed.	4.0	More Details
CVE-2025-43206	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7. An app may be able to access protected user data.	4.0	More Details
CVE-2025-43197	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sequoia 15.6, macOS Sonoma 14.7.7, macOS Ventura 13.7.7. An app may be able to access sensitive user data.	4.0	More Details
CVE-2025-44964	A lack of SSL certificate validation in BlueStacks v5.20 allows attackers to execute a man-it-the-middle attack and obtain sensitive information.	3.9	More Details
CVE-2025-54085	CVE-2025-54085 is a vulnerability in the management console of Absolute Secure Access prior to version 13.56. Attackers with administrative access to the console and who have been assigned a certain set of permissions can bypass those permissions to improperly read or change other settings. The attack complexity is low, there are no preexisting attack requirements; the privileges required are high, and there is no user interaction required. The impact to system confidentiality and integrity is low, there is no impact to system availability.	3.8	More Details
CVE-2025-46094	LiquidFiles before 4.1.2 allows directory traversal by configuring the pathname of a local executable file as an Actionscript.	3.8	More Details
CVE-2025-8548	A vulnerability was found in atjiu pybbs up to 6.0.0 and classified as problematic. This issue affects the function sendEmailCode of the file src/main/java/co/yiiu/pybbs/controller/api/SettingsApiController.java of the component Registered Email Handler. The manipulation of the argument email leads to information exposure through error message. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is 234197c4f8fc7ce24bdcff5430cd42492f28936a. It is recommended to apply a patch to fix this issue.	3.7	More Details
CVE-2025-54350	In iperf before 3.19.1, iperf_auth.c has a Base64Decode assertion failure and application exit upon a malformed authentication attempt.	3.7	More Details
CVE-2025-8549	A vulnerability was found in atjiu pybbs up to 6.0.0. It has been classified as critical. Affected is the function update of the file src/main/java/co/yiiu/pybbs/controller/admin/UserAdminController.java. The manipulation leads to weak password requirements. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The patch is identified as d09cb19a8e7d7e5151282926ada54080244d499f. It is recommended to apply a patch to fix this issue.	3.7	More Details
CVE-2025-6011	A timing side channel in Vault and Vault Enterprise’s (“Vault”) userpass auth method allowed an attacker to distinguish between existing and non-existing users, and potentially enumerate valid usernames for Vault’s Userpass auth method. Fixed in Vault Community Edition 1.20.1 and Vault Enterprise 1.20.1, 1.19.7, 1.18.12, and 1.16.23.	3.7	More Details
CVE-2025-8537	A vulnerability, which was classified as problematic, was found in Axiomatic Bento4 up to 1.6.0-641. Affected is the function AP4_DataBuffer::SetDataSize of the file Mp4Decrypt.cpp of the component mp4decrypt. The manipulation leads to allocation of resources. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used.	3.7	More Details
CVE-2025-8528	A vulnerability classified as problematic has been found in Exrick xboot up to 3.3.4. Affected is an unknown function of the file /xboot/permission/getMenuList. The manipulation leads to cleartext storage of sensitive information in a cookie. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used.	3.7	More Details

CVE-2023-32251	A vulnerability has been identified in the Linux kernel's ksmbd component (kernel SMB/CIFS server). A security control designed to prevent dictionary attacks, which introduces a 5-second delay during session setup, can be bypassed through the use of asynchronous requests. This bypass negates the intended anti-brute-force protection, potentially allowing attackers to conduct dictionary attacks more efficiently against user credentials or other authentication mechanisms.	3.7	More Details
CVE-2025-52567	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. In versions 0.84 through 10.0.18, usage of RSS feeds or external calendars when planning is subject to SSRF exploit. The previous security patches provided since GLPI 10.0.4 were not robust enough for certain specific cases. This is fixed in version 10.0.19.	3.5	More Details
CVE-2025-8509	A vulnerability was found in Portabilis i-Educar 2.9. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /intranet/educar_servidor_cad.php. The manipulation of the argument matricula leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-8510	A vulnerability classified as problematic has been found in Portabilis i-Educar 2.10. This affects the function Gerar of the file ieducar/intranet/educar_matricula_lst.php. The manipulation of the argument ref_cod_aluno leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 82c288b9a4abb084bdfa1c0c4ef777ed45f98b46. It is recommended to apply a patch to fix this issue. The vendor initially closed the original advisory without requesting a CVE.	3.5	More Details
CVE-2025-8511	A vulnerability classified as problematic was found in Portabilis i-Diario 1.5.0. This vulnerability affects unknown code of the file /diario-de-observacoes/ of the component Observações. The manipulation of the argument Descrição leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-8535	A vulnerability, which was classified as problematic, has been found in cronoh NanoVault up to 1.2.1. This issue affects the function executeJavaScript of the file /main.js of the component xrb URL Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-8506	A vulnerability was found in 495300897 wx-shop up to de1b66331368695779cfc6e4d11a64caddf8716e and classified as problematic. This issue affects some unknown processing of the file /user/editUI. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may 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.	3.5	More Details
CVE-2025-51383	D-LINK DI-8200 16.07.26A1 is vulnerable to Buffer Overflow in the ipsec_road_asp function via the host_ip parameter.	3.5	More Details
CVE-2025-8380	A vulnerability classified as problematic was found in Campcodes Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /admin/add_query_account.php. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-51384	D-LINK DI-8200 16.07.26A1 is vulnerable to Buffer Overflow in the ipsec_net_asp function via the remot_ip parameter.	3.5	More Details
CVE-2025-8507	A vulnerability was found in Portabilis i-Educar 2.9. It has been classified as problematic. Affected is an unknown function of the file /intranet/educar_funcao_lst.php. The manipulation of the argument nm_funcao/abreviatura leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-8508	A vulnerability was found in Portabilis i-Educar 2.9. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /intranet/educar_avaliacao_desempenho_cad.php. The manipulation of the argument titulo_avaliacao/descricao leads to cross site scripting. The attack can be launched remotely. The	3.5	More Details

	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.		
CVE-2025-51385	D-LINK DI-8200 16.07.26A1 is vulnerable to Buffer Overflow in the yyxz_dlink_asp function via the id parameter.	3.5	More Details
CVE-2025-8365	A vulnerability was found in Portabilis i-Educar 2.10. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file atendidos_cad.php. The manipulation of the argument nome/nome_social/email leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-8551	A vulnerability was found in atjiu pybbs up to 6.0.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/comment/list. The manipulation of the argument Username leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2025-37109	Cross-site scripting vulnerability has been identified in HPE Telco Service Activator product	3.5	More Details
CVE-2025-8555	A vulnerability, which was classified as problematic, was found in atjiu pybbs up to 6.0.0. Affected is an unknown function of the file /search. The manipulation of the argument keyword leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2025-8501	A vulnerability classified as problematic has been found in code-projects Human Resource Integrated System 1.0. Affected is an unknown function of the file /insert-and-view/action.php. The manipulation of the argument content leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-37108	Cross-site scripting vulnerability has been identified in HPE Telco Service Activator product	3.5	More Details
CVE-2025-8584	A vulnerability classified as problematic was found in libav up to 12.3. Affected by this vulnerability is the function av_buffer_unref of the file libavutil/buffer.c of the component AVI File Parser. The manipulation leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The bug was initially reported by the researcher to the wrong project. This vulnerability only affects products that are no longer supported by the maintainer.	3.3	More Details
CVE-2025-23287	NVIDIA GPU Display Driver for Windows contains a vulnerability where an attacker may access sensitive system-level information. A successful exploit of this vulnerability may lead to Information disclosure.	3.3	More Details
CVE-2025-23288	NVIDIA GPU Display Driver for Windows contains a vulnerability where an attacker may cause an exposure of sensitive system information with local unprivileged system access. A successful exploit of this vulnerability may lead to Information disclosure.	3.3	More Details
CVE-2025-8586	A vulnerability, which was classified as problematic, was found in libav up to 12.3. This affects the function ff_seek_frame_binary of the file /libavformat/utils.c of the component MPEG File Parser. The manipulation leads to null pointer dereference. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The bug was initially reported by the researcher to the wrong project. This vulnerability only affects products that are no longer supported by the maintainer.	3.3	More Details
CVE-2025-54410	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker Engine, Mirantis Container Runtime, and various other downstream projects/products. A firewalld vulnerability affects Moby releases before 28.0.0. When firewalld reloads, Docker fails to re-create iptables rules that isolate bridge networks, allowing any container to access all ports on any other container across different bridge networks on the same host. This breaks network segmentation between containers that should be isolated, creating significant risk in multi-tenant environments. Only containers in --internal networks remain protected. Workarounds include reloading firewalld and either restarting the docker daemon, re-creating bridge networks, or using rootless mode.	3.3	More Details

	Maintainers anticipate a fix for this issue in version 25.0.13.		
CVE-2023-44976	Hangzhou Shunwang Rentdrv2 before 2024-12-24 allows local users to terminate EDR processes and possibly have unspecified other impact via DeviceIoControl with control code 0x22E010, as exploited in the wild in October 2023.	3.2	More Details
CVE-2025-54956	The gh package before 1.5.0 for R delivers an HTTP response in a data structure that includes the Authorization header from the corresponding HTTP request.	3.2	More Details
CVE-2025-8515	A vulnerability was found in Intelbras InControl 2.21.60.9 and classified as problematic. This issue affects some unknown processing of the file /v1/operador/ of the component JSON Endpoint. The manipulation leads to information disclosure. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component.	3.1	More Details
CVE-2025-54781	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. When debugging is enabled for Himmelblau in version 1.0.0, the himmelblaud_tasks service leaks an Intune service access token to the system journal. This short-lived token can be used to detect the host's Intune compliance status, and may permit additional administrative operations for the Intune host device (though the API for these operations is undocumented). This is fixed in version 1.1.0. To workaround this issue, ensure that Himmelblau debugging is disabled.	2.8	More Details
CVE-2025-8519	A vulnerability classified as problematic has been found in givanz Vvveb up to 1.0.5. This affects an unknown part of the file /vadmin123/index.php?module=editor/editor of the component Drag-and-Drop Editor. The manipulation of the argument url leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.6 is able to address this issue. The identifier of the patch is f684f3e374d04db715730fc4796e102f5ebcacb2. It is recommended to upgrade the affected component.	2.7	More Details
CVE-2025-53113	GLPI, which stands for Gestionnaire Libre de Parc Informatique, is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions 0.65 through 10.0.18, a technician can use the external links feature to fetch information on items they do not have the right to see. This is fixed in version 10.0.19.	2.7	More Details
CVE-2025-49082	CVE-2025-49082 is a vulnerability in the management console of Absolute Secure Access prior to version 13.56. Attackers with administrative access to the console and who have been assigned a certain set of permissions can bypass those permissions to improperly read other settings. The attack complexity is low, there are no preexisting attack requirements; the privileges required are high, and there is no user interaction required. The impact to system confidentiality is low, there is no impact to system availability or integrity.	2.7	More Details
CVE-2025-8534	A vulnerability classified as problematic was found in libtiff 4.6.0. This vulnerability affects the function PS_Lvl2page of the file tools/tiff2ps.c of the component tiff2ps. The manipulation leads to null pointer dereference. It is possible to launch the attack on the local host. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The name of the patch is 6ba36f159fd396ad11bf6b7874554197736ecc8b. It is recommended to apply a patch to fix this issue. One of the maintainers explains, that "[t]his error only occurs if DEFER_STRILE_LOAD (defer-strile-load:BOOL=ON) or TIFFOpen(.. "rD") option is used."	2.5	More Details
CVE-2025-23290	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a guest could get global GPU metrics which may be influenced by work in other VMs. A successful exploit of this vulnerability might lead to information disclosure.	2.5	More Details
CVE-2025-36609	Dell SmartFabric OS10 Software, versions prior to 10.6.0.5, contains a Use of Hard-coded Password vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2.5	More Details
CVE-2024-13978	A vulnerability was found in LibTIFF up to 4.7.0. It has been declared as problematic. Affected by this vulnerability is the function t2p_read_tiff_init of the file tools/tiff2pdf.c of the component fax2ps. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The complexity of an attack is rather high. The exploitation appears to be difficult. The patch is named 2ebfffb0e8836bfb1cd7d85c059cd285c59761a4. It is recommended to apply a patch to fix this issue.	2.5	More Details
CVE-	A vulnerability was found in atjiu pybbs up to 6.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/topic/list. The manipulation of the		

2025-8550	argument Username leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The patch is named 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to fix this issue.	2.4	More Details
CVE-2025-8552	A vulnerability classified as problematic has been found in atjiu pybbs up to 6.0.0. This affects an unknown part of the file /admin/tag/list. The manipulation of the argument Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to fix this issue.	2.4	More Details
CVE-2025-8553	A vulnerability classified as problematic was found in atjiu pybbs up to 6.0.0. This vulnerability affects unknown code of the file /admin/sensitive_word/list. The manipulation of the argument word leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to fix this issue.	2.4	More Details
CVE-2025-8521	A vulnerability, which was classified as problematic, has been found in givanz Vvveb up to 1.0.5. This issue affects some unknown processing of the file /vadmin123/index.php?module=settings/post-types of the component Add Type Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.6 is able to address this issue. The patch is named b53c7161da606f512b7efcb392d6ffc708688d49/605a70f8729e4d44ebe272671cb1e43e3d6ae014. It is recommended to upgrade the affected component.	2.4	More Details
CVE-2025-8554	A vulnerability, which was classified as problematic, has been found in atjiu pybbs up to 6.0.0. This issue affects some unknown processing of the file /admin/user/list. The manipulation of the argument Username leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is named 2fe4a51afbce0068c291bc1818bbc8f7f3b01a22. It is recommended to apply a patch to fix this issue.	2.4	More Details
CVE-2025-8545	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.10. Affected by this issue is some unknown functionality of the file /intranet/educar_motivo_afastamento_cad.php. The manipulation of the argument nm_motivo leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8538	A vulnerability has been found in Portabilis i-Educar 2.10 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /usuarios/tipos/novo. The manipulation of the argument name/description leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8539	A vulnerability was found in Portabilis i-Educar 2.10 and classified as problematic. Affected by this issue is some unknown functionality of the file /intranet/public_distrito_cad.php. The manipulation of the argument nome leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8540	A vulnerability was found in Portabilis i-Educar 2.10. It has been classified as problematic. This affects an unknown part of the file /intranet/public_municipio_cad.php. The manipulation of the argument nome leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8541	A vulnerability was found in Portabilis i-Educar 2.10. It has been declared as problematic. This vulnerability affects unknown code of the file /intranet/public_uf_cad.php. The manipulation of the argument nome leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8544	A vulnerability classified as problematic was found in Portabilis i-Educar 2.10. Affected by this vulnerability is an unknown functionality of the file /module/RegraAvaliacao/edit. The manipulation of the argument nome leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details

CVE-2025-8543	A vulnerability classified as problematic has been found in Portabilis i-Educar 2.10. Affected is an unknown function of the file /intranet/educar_raca_cad.php. The manipulation of the argument nm_raca leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8542	A vulnerability was found in Portabilis i-Educar 2.10. It has been rated as problematic. This issue affects some unknown processing of the file /intranet/empresas_cad.php. The manipulation of the argument fantasia/razao_social leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-8337	A vulnerability, which was classified as problematic, has been found in code-projects Simple Car Rental System 1.0. This issue affects some unknown processing of the file /admin/add_vehicles.php. The manipulation of the argument car_name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2025-53534	RatPanel is a server operation and maintenance management panel. In versions 2.3.19 through 2.5.5, when an attacker obtains the backend login path of RatPanel (including but not limited to weak default paths, brute-force cracking, etc.), they can execute system commands or take over hosts managed by the panel without logging in. In addition to this remote code execution (RCE) vulnerability, the flawed code also leads to unauthorized access. RatPanel uses the CleanPath middleware provided by github.com/go-chi/chi package to clean URLs, but but the middleware does not process r.URL.Path, which can cause the paths to be misinterpreted. This is fixed in version 2.5.6.	N/A	More Details
CVE-2025-54976	Rejected reason: Not used	N/A	More Details
CVE-2025-53417	DIAView (v4.2.0 and prior) - Directory Traversal Information Disclosure Vulnerability	N/A	More Details
CVE-2025-54974	Rejected reason: Not used	N/A	More Details
CVE-2025-54975	Rejected reason: Not used	N/A	More Details
CVE-2025-8571	Concrete CMS 9 to 9.4.2 and versions below 8.5.21 are vulnerable to Reflected Cross-Site Scripting (XSS) in the Conversation Messages Dashboard Page. Unsanitized input could cause theft of session cookies or tokens, defacement of web content, redirection to malicious sites, and (if victim is an admin), the execution of unauthorized actions. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks Fortbridge https://fortbridge.co.uk/ for performing a penetration test and vulnerability assessment on Concrete CMS and reporting this issue.	N/A	More Details
CVE-2025-54979	Rejected reason: Not used	N/A	More Details
CVE-2025-54977	Rejected reason: Not used	N/A	More Details
CVE-2025-54978	Rejected reason: Not used	N/A	More Details
CVE-2025-54980	Rejected reason: Not used	N/A	More Details
CVE-	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and		More

2025-41375	delete databases through the 'idestudio' parameter in /encuestas/integraweb[_v4]/integra/html/view/consultaincimails.php.	N/A	Details
CVE-2025-53399	In Sipwise rtpengine before 13.4.1.1, an origin-validation error in the endpoint-learning logic of the media-relay core allows remote attackers to inject or intercept RTP/SRTP media streams via RTP packets (except when the relay is configured for strict source and learning disabled). Version 13.4.1.1 fixes the heuristic mode by limiting exposure to the first five packets, and introduces a recrypt flag that fully prevents SRTP attacks when both mitigations are enabled.	N/A	More Details
CVE-2025-48074	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In version 3.3.2, applications trust unvalidated dataWindow size values from file headers, which can lead to excessive memory allocation and performance degradation when processing malicious files. This is fixed in version 3.3.3.	N/A	More Details
CVE-2025-48071	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.3.2 through 3.3.0, there is a heap-based buffer overflow during a write operation when decompressing ZIPS-packed deep scan-line EXR files with a maliciously forged chunk header. This is fixed in version 3.3.3.	N/A	More Details
CVE-2025-48072	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. Version 3.3.2 is vulnerable to a heap-based buffer overflow during a read operation due to bad pointer math when decompressing DWAA-packed scan-line EXR files with a maliciously forged chunk. This is fixed in version 3.3.3.	N/A	More Details
CVE-2025-48073	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In version 3.3.2, when reading a deep scanline image with a large sample count in reduceMemory mode, it is possible to crash a target application with a NULL pointer dereference in a write operation. This is fixed in version 3.3.3.	N/A	More Details
CVE-2025-41376	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and delete databases through the 'idestudio' parameter in /encuestas/integraweb[_v4]/integra/html/view/consultacuotasred.php.	N/A	More Details
CVE-2013-10070	PHP-Charts v1.0 contains a PHP code execution vulnerability in wizard/url.php, where user-supplied GET parameter names are passed directly to eval() without sanitization. A remote attacker can exploit this flaw by crafting a request that injects arbitrary PHP code, resulting in command execution under the web server's context. The vulnerability allows unauthenticated attackers to execute system-level commands via base64-encoded payloads embedded in parameter names, leading to full compromise of the host system.	N/A	More Details
CVE-2025-41374	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and delete databases through the 'idestudio' parameter in /encuestas/integraweb[_v4]/integra/html/view/hislistadoacciones.php.	N/A	More Details
CVE-2012-10032	Maxthon3 versions prior to 3.3 are vulnerable to cross context scripting (XCS) via the about:history page. The browser’s trusted zone improperly handles injected script content, allowing attackers to execute arbitrary JavaScript in a privileged context. This flaw enables modification of browser configuration and execution of arbitrary code through Maxthon’s exposed DOM APIs, including maxthon.program.Program.launch() and maxthon.io.writeDataURL(). Exploitation requires user interaction, typically by visiting a malicious webpage that triggers the injection.	N/A	More Details
CVE-2012-10024	XBMC version 11, including builds up to the 2012-11-04 nightly release, contains a path traversal vulnerability in its embedded HTTP server. When accessed via HTTP Basic Authentication, the server fails to properly sanitize URI input, allowing authenticated users to request files outside the intended document root. An attacker can exploit this flaw to read arbitrary files from the host filesystem, including sensitive configuration or credential files.	N/A	More Details
CVE-2012-10025	The WordPress plugin Advanced Custom Fields (ACF) version 3.5.1 and below contains a remote file inclusion (RFI) vulnerability in core/actions/export.php. When the PHP configuration directive allow_url_include is enabled (default: Off), an unauthenticated attacker can exploit the acf_abspath POST parameter to include and execute arbitrary remote PHP code. This leads to remote code execution under the web server’s context, allowing full compromise of the host.	N/A	More Details
CVE-	The WordPress plugin Asset-Manager version 2.0 and below contains an unauthenticated arbitrary file upload vulnerability in upload.php. The endpoint fails to properly validate and restrict uploaded		More

2012-10026	file types, allowing remote attackers to upload malicious PHP scripts to a predictable temporary directory. Once uploaded, the attacker can execute the file via a direct HTTP GET request, resulting in remote code execution under the web server’s context.	N/A	Details
CVE-2012-10027	WP-Property plugin for WordPress through version 1.35.0 contains an unauthenticated file upload vulnerability in the third-party \`uploadify.php\` script. A remote attacker can upload arbitrary PHP files to a temporary directory without authentication, leading to remote code execution.	N/A	More Details
CVE-2012-10028	Netwin SurgeFTP version 23c8 and prior contains a vulnerability in its web-based administrative console that allows authenticated users to execute arbitrary system commands via crafted POST requests to \`surgeftpmgr.cgi\`. This can lead to full remote code execution on the underlying system.	N/A	More Details
CVE-2012-10029	Nagios XI Network Monitor prior to Graph Explorer component version 1.3 contains a command injection vulnerability in \`visApi.php\`. An authenticated user can inject system commands via unsanitized parameters such as \`host\`, resulting in remote code execution.	N/A	More Details
CVE-2012-10030	FreeFloat FTP Server contains multiple critical design flaws that allow unauthenticated remote attackers to upload arbitrary files to sensitive system directories. The server accepts empty credentials, defaults user access to the root of the C:\ drive, and imposes no restrictions on file type or destination path. These conditions enable attackers to upload executable payloads and .mof files to locations such as system32 and wbem\mof, where Windows Management Instrumentation (WMI) automatically processes and executes them. This results in remote code execution with SYSTEM-level privileges, without requiring user interaction.	N/A	More Details
CVE-2012-10031	BlazeVideo HDTV Player Pro v6.6.0.3 is vulnerable to a stack-based buffer overflow due to improper handling of user-supplied input embedded in .plf playlist files. When parsing a crafted .plf file, the MediaPlayerCtrl.dll component invokes PathFindFileNameA() to extract a filename from a URL-like string. The returned value is then copied to a fixed-size stack buffer using an inline strcpy call without bounds checking. If the input exceeds the buffer size, this leads to a stack overflow and potential arbitrary code execution under the context of the user.	N/A	More Details
CVE-2012-10033	Narcissus is vulnerable to remote code execution via improper input handling in its image configuration workflow. Specifically, the backend.php script fails to sanitize the release parameter before passing it to the configure_image() function. This function invokes PHP’s passthru() with the unsanitized input, allowing attackers to inject arbitrary system commands. Exploitation occurs via a crafted POST request, resulting in command execution under the web server’s context.	N/A	More Details
CVE-2025-54844	Rejected reason: Not used	N/A	More Details
CVE-2012-10034	ClanSphere 2011.3 is vulnerable to a local file inclusion (LFI) flaw due to improper handling of the cs_lang cookie parameter. The application fails to sanitize user-supplied input, allowing attackers to traverse directories and read arbitrary files outside the web root. The vulnerability is further exacerbated by null byte injection (%00) to bypass file extension checks.	N/A	More Details
CVE-2012-10035	Turbo FTP Server versions 1.30.823 and 1.30.826 contain a buffer overflow vulnerability in the handling of the PORT command. By sending a specially crafted payload, an unauthenticated remote attacker can overwrite memory structures and execute arbitrary code with SYSTEM privileges.	N/A	More Details
CVE-2013-10064	A stack-based buffer overflow vulnerability exists in ActFax Server version 5.01. The server's RAW protocol interface fails to safely process user-supplied data in @F506 fax header fields due to insecure usage of strcpy. Remote attackers can exploit this vulnerability by sending specially crafted @F506 fields, potentially leading to arbitrary code execution. Successful exploitation requires network access to TCP port 4559 and does not require authentication.	N/A	More Details
CVE-2013-10065	A denial-of-service vulnerability exists in Sysax Multi-Server version 6.10 via its SSH daemon. A specially crafted SSH key exchange packet can trigger a crash in the service, resulting in loss of availability. The flaw is triggered during the handling of malformed key exchange data, including a non-standard byte (\x28) in place of the expected SSH protocol delimiter.	N/A	More Details
CVE-2013-10066	An unauthenticated arbitrary file upload vulnerability exists in Kordil EDMS v2.2.60rc3. The application exposes an upload endpoint (users_add.php) that allows attackers to upload files to the /userpictures/ directory without authentication. This flaw enables remote code execution by uploading a PHP payload and invoking it via a direct HTTP request.	N/A	More Details
CVE-2013-	Glossword versions 1.8.8 through 1.8.12 contain an authenticated arbitrary file upload vulnerability. When deployed as a standalone application, the administrative interface (gw_admin.php) allows users with administrator privileges to upload files to the gw_temp/a/ directory. Due to insufficient	N/A	More

10067	validation of file type and path, attackers can upload and execute PHP payloads, resulting in remote code execution.		Details
CVE-2013-10068	Foxit Reader Plugin version 2.2.1.530, bundled with Foxit Reader 5.4.4.11281, contains a stack-based buffer overflow vulnerability in the npFoxitReaderPlugin.dll module. When a PDF file is loaded from a remote host, an overly long query string in the URL can overflow a buffer, allowing remote attackers to execute arbitrary code.	N/A	More Details
CVE-2013-10069	The web interface of multiple D-Link routers, including DIR-600 rev B (≤2.14b01) and DIR-300 rev B (≤2.13), contains an unauthenticated OS command injection vulnerability in command.php, which improperly handles the cmd POST parameter. A remote attacker can exploit this flaw without authentication to spawn a Telnet service on a specified port, enabling persistent interactive shell access as root.	N/A	More Details
CVE-2012-10023	A stack-based buffer overflow vulnerability exists in FreeFloat FTP Server version 1.0.0. The server fails to properly validate input passed to the USER command, allowing remote attackers to overwrite memory and potentially execute arbitrary code. The flaw is triggered by sending an overly long username string, which overflows the buffer allocated for user authentication.	N/A	More Details
CVE-2025-54845	Rejected reason: Not used	N/A	More Details
CVE-2025-41373	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and delete databases through the 'idestudio' parameter in /encuestas/integraweb[_v4]/integra/html/view/hislistadoacciones.php.	N/A	More Details
CVE-2025-54657	Rejected reason: Not used	N/A	More Details
CVE-2025-7025	A memory abuse issue exists in the Rockwell Automation Arena® Simulation. A custom file can force Arena Simulation to read and write past the end of memory space. Successful use requires user action, such as opening a bad file or webpage. If used, a threat actor could execute code or disclose information.	N/A	More Details
CVE-2025-7032	A memory abuse issue exists in the Rockwell Automation Arena® Simulation. A custom file can force Arena Simulation to read and write past the end of memory space. Successful use requires user action, such as opening a bad file or webpage. If used, a threat actor could execute code or disclose information.	N/A	More Details
CVE-2025-7033	A memory abuse issue exists in the Rockwell Automation Arena® Simulation. A custom file can force Arena Simulation to read and write past the end of memory space. Successful use requires user action, such as opening a bad file or webpage. If used, a threat actor could execute code or disclose information.	N/A	More Details
CVE-2025-41372	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and delete databases through the 'idestudio' parameter in /encuestas/integraweb[_v4]/integra/html/view/informe_campo_entrevistas.php.	N/A	More Details
CVE-2014-125113	An unrestricted file upload vulnerability exists in Dell (acquired by Quest) KACE K1000 System Management Appliance version 5.0 - 5.3, 5.4 prior to 5.4.76849, and 5.5 prior to 5.5.90547 in the download_agent.php endpoint. An attacker can upload arbitrary PHP files to a temporary web-accessible directory, which are later executed through inclusion in backend code that loads files under attacker-controlled paths.	N/A	More Details
CVE-2025-2611	The ICTBroadcast application unsafely passes session cookie data to shell processing, allowing an attacker to inject shell commands into a session cookie that get executed on the server. This results in unauthenticated remote code execution in the session handling. Versions 7.4 and below are known to be vulnerable.	N/A	More Details
CVE-2025-54847	Rejected reason: Not used	N/A	More Details

CVE-2025-41370	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and delete databases through the 'idestudio' parameter in /encuestas/integraweb/html/view/acceso.php.	N/A	More Details
CVE-2025-54874	OpenJPEG is an open-source JPEG 2000 codec. In OpenJPEG 2.5.3 and earlier, a call to opj_jp2_read_header may lead to OOB heap memory write when the data stream p_stream is too short and p_image is not initialized.	N/A	More Details
CVE-2025-54843	Rejected reason: Not used	N/A	More Details
CVE-2025-54839	Rejected reason: Not used	N/A	More Details
CVE-2025-54840	Rejected reason: Not used	N/A	More Details
CVE-2025-54846	Rejected reason: Not used	N/A	More Details
CVE-2025-7674	Improper Input Validation vulnerability in Roche Diagnostics navify Monitoring allows an attacker to manipulate input data, which may lead to a denial of service (DoS) due to negatively impacting the server's performance. This vulnerability has no impact on data confidentiality or integrity. This issue affects navify Monitoring before 1.08.00.	N/A	More Details
CVE-2025-6398	A null pointer dereference vulnerability exists in the IOMap64.sys driver of ASUS AI Suite 3. The vulnerability can be triggered by a specially crafted input, which may lead to a system crash (BSOD). Refer to the ' Security Update for for AI Suite 3 ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-54841	Rejected reason: Not used	N/A	More Details
CVE-2025-54842	Rejected reason: Not used	N/A	More Details
CVE-2025-51541	A stored cross-site scripting (XSS) vulnerability exists in the Shopware 6 installation interface at /recovery/install/database-configuration/. The c_database_schema field fails to properly sanitize user-supplied input before rendering it in the browser, allowing an attacker to inject malicious JavaScript. This vulnerability can be exploited via a Cross-Site Request Forgery (CSRF) attack due to the absence of CSRF protections on the POST request. An unauthenticated remote attacker can craft a malicious web page that, when visited by a victim, stores the payload persistently in the installation configuration. As a result, the payload executes whenever any user subsequently accesses the vulnerable installation page, leading to persistent client-side code execution.	N/A	More Details
CVE-2025-41371	A SQL injection vulnerability has been found in Gandia Integra Total of TESI from version 2.1.2217.3 to v4.4.2236.1. The vulnerability allows an authenticated attacker to retrieve, create, update and delete databases through the 'idestudio' parameter in /encuestas/integraweb_v4/integra/html/view/acceso.php	N/A	More Details
CVE-2011-10008	A stack-based buffer overflow vulnerability exists in MPlayer Lite r33064 due to improper bounds checking when handling M3U playlist files containing long http:// URL entries. An attacker can craft a malicious .m3u file with a specially formatted URL that triggers a stack overflow when processed by the player, particularly via drag-and-drop interaction. This flaw allows for control of the execution flow through SEH overwrite and a DEP bypass using a ROP chain that leverages known gadgets in loaded DLLs. Successful exploitation may result in arbitrary code execution with the privileges of the current user.	N/A	More Details
CVE-2025-54870	VTun-ng is a Virtual Tunnel over TCP/IP network. In versions 3.0.17 and below, failure to initialize encryption modules might cause reversion to plaintext due to insufficient error handling. The bug was first introduced in VTun-ng version 3.0.12. This is fixed in version 3.0.18. To workaround this issue, avoid blowfish-256.	N/A	More Details

CVE-2025-54828	Rejected reason: Not used	N/A	More Details
CVE-2025-54789	Files is a module for managing files inside spaces and user profiles. In versions 0.16.9 and below, the File Move functionality does not contain logic that prevents injection of arbitrary JavaScript, which can lead to Browser JS code execution in the context of the user's session. This is fixed in version 0.16.10.	N/A	More Details
CVE-2025-54782	Nest is a framework for building scalable Node.js server-side applications. In versions 0.2.0 and below, a critical Remote Code Execution (RCE) vulnerability was discovered in the @nestjs/devtools-integration package. When enabled, the package exposes a local development HTTP server with an API endpoint that uses an unsafe JavaScript sandbox (safe-eval-like implementation). Due to improper sandboxing and missing cross-origin protections, any malicious website visited by a developer can execute arbitrary code on their local machine. The package adds HTTP endpoints to a locally running NestJS development server. One of these endpoints, /inspector/graph/interact, accepts JSON input containing a code field and executes the provided code in a Node.js vm.runInNewContext sandbox. This is fixed in version 0.2.1.	N/A	More Details
CVE-2025-54827	Rejected reason: Not used	N/A	More Details
CVE-2025-54826	Rejected reason: Not used	N/A	More Details
CVE-2025-54825	Rejected reason: Not used	N/A	More Details
CVE-2025-54824	Rejected reason: Not used	N/A	More Details
CVE-2025-54386	Traefik is an HTTP reverse proxy and load balancer. In versions 2.11.27 and below, 3.0.0 through 3.4.4 and 3.5.0-rc1, a path traversal vulnerability was discovered in WASM Traefik's plugin installation mechanism. By supplying a maliciously crafted ZIP archive containing file paths with ../ sequences, an attacker can overwrite arbitrary files on the system outside of the intended plugin directory. This can lead to remote code execution (RCE), privilege escalation, persistence, or denial of service. This is fixed in versions 2.11.28, 3.4.5 and 3.5.0.	N/A	More Details
CVE-2025-54823	Rejected reason: Not used	N/A	More Details
CVE-2023-41674	Rejected reason: Not used	N/A	More Details
CVE-2025-54133	Cursor is a code editor built for programming with AI. In versions 1.17 through 1.2, there is a UI information disclosure vulnerability in Cursor's MCP (Model Context Protocol) deeplink handler, allowing attackers to execute 2-click arbitrary system commands through social engineering attacks. When users click malicious `cursor://anysphere.cursor-deeplink/mcp/install` links, the installation dialog does not show the arguments being passed to the command being run. If a user clicks a malicious deeplink, then examines the installation dialog and clicks through, the full command including the arguments will be executed on the machine. This is fixed in version 1.3.	N/A	More Details
CVE-2025-54792	LocalSend is an open-source app to securely share files and messages with nearby devices over local networks without needing an internet connection. In versions 1.16.1 and below, a critical Man-in-the-Middle (MitM) vulnerability in the software's discovery protocol allows an unauthenticated attacker on the same local network to impersonate legitimate devices, silently intercepting, reading, and modifying any file transfer. This can be used to steal sensitive data or inject malware, like ransomware, into files shared between trusted users. The attack is hardly detectable and easy to implement, posing a severe and immediate security risk. This issue was fixed in version 1.17.0.	N/A	More Details
CVE-2013-	A path traversal vulnerability exists in the Netgear SPH200D Skype phone firmware versions <= 1.0.4.80 in its embedded web server. Authenticated attackers can exploit crafted GET requests to	N/A	More

10063	access arbitrary files outside the web root by injecting traversal sequences. This can expose sensitive system files and configuration data.		Details
CVE-2013-10062	A directory traversal vulnerability exists in Linksys router's web interface (tested on the E1500 model firmware versions 1.0.00, 1.0.04, and 1.0.05), specifically in the /apply.cgi endpoint. Authenticated attackers can exploit the next_page POST parameter to access arbitrary files outside the intended web root by injecting traversal sequences. This allows exposure of sensitive system files and configuration data.	N/A	More Details
CVE-2025-7356	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-11478	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2013-10061	An authenticated OS command injection vulnerability exists in Netgear routers (tested on the DGN1000B model firmware versions 1.1.00.24 and 1.1.00.45) via the TimeToLive parameter in the setup.cgi endpoint. The vulnerability arises from improper input neutralization, enabling command injection through crafted POST requests. This flaw enables remote attackers to deploy payloads or manipulate system state post-authentication.	N/A	More Details
CVE-2013-10060	An authenticated OS command injection vulnerability exists in Netgear routers (tested on the DGN2200B model) firmware versions 1.0.0.36 and prior via the pppoe.cgi endpoint. A remote attacker with valid credentials can execute arbitrary commands via crafted input to the pppoe_username parameter. This flaw allows full compromise of the device and may persist across reboots unless configuration is restored.	N/A	More Details
CVE-2025-54582	Rejected reason: Reason: This candidate was issued in error. Valid Netty requests are issued via https://github.com/netty/netty.	N/A	More Details
CVE-2013-10059	An authenticated OS command injection vulnerability exists in various D-Link routers (tested on DIR-615H1 running firmware version 8.04) via the tools_vct.htm endpoint. The web interface fails to sanitize input passed from the ping_ipaddr parameter to the tools_vct.htm diagnostic interface, allowing attackers to inject arbitrary shell commands using backtick encapsulation. With default credentials, an attacker can exploit this blind injection vector to execute arbitrary commands.	N/A	More Details
CVE-2025-54790	Files is a module for managing files inside spaces and user profiles. In versions 0.16.9 and below, Files does not have logic to prevent the exploitation of backend SQL queries without direct output, potentially allowing unauthorized data access. This is fixed in version 0.16.10.	N/A	More Details
CVE-2025-34146	A prototype pollution vulnerability exists in @nyariv/sandboxjs versions <= 0.8.23, allowing attackers to inject arbitrary properties into Object.prototype via crafted JavaScript code. This can result in a denial-of-service (DoS) condition or, under certain conditions, escape the sandboxed environment intended to restrict code execution. The vulnerability stems from insufficient prototype access checks in the sandbox's executor logic, particularly in the handling of JavaScript function objects returned.	N/A	More Details
CVE-2025-8426	Marvell QConvergeConsole compressConfigFiles Directory Traversal Information Disclosure and Denial-of-Service Vulnerability. This vulnerability allows remote attackers to disclose sensitive information or to create a denial-of-service condition on affected installations of Marvell QConvergeConsole. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the compressConfigFiles method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose sensitive information or to create a denial-of-service condition on the system. Was ZDI-CAN-24915.	N/A	More Details
CVE-2025-54829	Rejected reason: Not used	N/A	More Details
CVE-2013-10033	An unauthenticated SQL injection vulnerability exists in Kimai version 0.9.2.x via the db_restore.php endpoint. The flaw allows attackers to inject arbitrary SQL queries into the dates[] POST parameter, enabling file write via INTO OUTFILE under specific environmental conditions. This can lead to remote code execution by writing a PHP payload to the web-accessible temporary directory. The vulnerability has been confirmed in versions including 0.9.2.beta, 0.9.2.1294.beta, and 0.9.2.1306-3.	N/A	More Details

CVE-2013-10034	An unrestricted file upload vulnerability exists in Kaseya KServer versions prior to 6.3.0.2. The uploadImage.asp endpoint allows unauthenticated users to upload files to arbitrary paths via a crafted filename parameter in a multipart/form-data POST request. Due to the lack of authentication and input sanitation, an attacker can upload a file with an .asp extension to a web-accessible directory, which can then be invoked to execute arbitrary code with the privileges of the IUSR account. The vulnerability enables remote code execution without prior authentication and was resolved in version 6.3.0.2 by removing the vulnerable uploadImage.asp endpoint.	N/A	More Details
CVE-2013-10035	A code injection vulnerability exists in ProcessMaker Open Source versions 2.x when using the default 'neoclassic' skin. An authenticated user can execute arbitrary PHP code via multiple endpoints, including appFolderAjax.php, casesStartPage_Ajax.php, and cases_SchedulerGetPlugins.php, by supplying crafted POST requests to parameters such as action and params. These endpoints fail to validate user input and directly invoke PHP functions like system() with user-supplied parameters, enabling remote code execution. The vulnerability affects both Linux and Windows installations and is present in default configurations of versions including 2.0.23 through 2.5.1. The vulnerable skin cannot be removed through the web interface, and exploitation requires only valid user credentials.	N/A	More Details
CVE-2013-10036	A stack-based buffer overflow vulnerability exists in Beetel Connection Manager version PCW_BTLINDV1.0.0B04 when parsing the UserName parameter in the NetConfig.ini configuration file. A crafted .ini file containing an overly long UserName value can overwrite the Structured Exception Handler (SEH), leading to arbitrary code execution when the application processes the file.	N/A	More Details
CVE-2013-10037	An OS command injection vulnerability exists in WebTester version 5.x via the install2.php installation script. The parameters cpusername, cppassword, and cpdomain are passed directly to shell commands without sanitization. A remote unauthenticated attacker can exploit this flaw by sending a crafted HTTP POST request, resulting in arbitrary command execution on the underlying system with web server privileges.	N/A	More Details
CVE-2013-10038	An unauthenticated arbitrary file upload vulnerability exists in FlashChat versions 6.0.2 and 6.0.4 through 6.0.8. The upload.php endpoint fails to properly validate file types and authentication, allowing attackers to upload malicious PHP scripts. Once uploaded, these scripts can be executed remotely, resulting in arbitrary code execution as the web server user.	N/A	More Details
CVE-2025-40980	A Stored Cross Site Scripting vulnerability has been found in UltimatePOS by UltimateFosters. This vulnerability is due to the lack of proper validation of user inputs via ‘/products/<PRODUCT_ID>/edit’, affecting to ‘name’ parameter via POST. The vulnerability could allow a remote attacker to send a specially crafted query to an authenticated user and steal his/her session cookies details.	N/A	More Details
CVE-2025-8192	There exists a TOCTOU race condition in TvSettings AppRestrictionsFragment.java that lead to start of attacker supplied activity in Settings’ context, i.e. system-uid context, thus lead to launchAnyWhere. The core idea is to utilize the time window between the check of Intent and the use to Intent to change the target component’s state, thus bypass the original security sanitize function.	N/A	More Details
CVE-2013-10039	A command injection vulnerability exists in GestioIP 3.0 commit ac67be and earlier in ip_checkhost.cgi. Crafted input to the 'ip' parameter allows attackers to execute arbitrary shell commands on the server via embedded base64-encoded payloads. Authentication may be required depending on deployment configuration.	N/A	More Details
CVE-2013-10040	ClipBucket version 2.6 and earlier contains a critical vulnerability in the ofc_upload_image.php script located at /admin_area/charts/ofc-library/. This endpoint allows unauthenticated users to upload arbitrary files, including executable PHP scripts. Once uploaded, the attacker can access the file via a predictable path and trigger remote code execution.	N/A	More Details
CVE-2013-10042	A stack-based buffer overflow vulnerability exists in freeFTPd version 1.0.10 and earlier in the handling of the FTP PASS command. When an attacker sends a specially crafted password string, the application fails to validate input length, resulting in memory corruption. This can lead to denial of service or arbitrary code execution. Exploitation requires the anonymous user account to be enabled.	N/A	More Details
CVE-2013-10043	A vulnerability exists in OAstium VoIP PBX astium-confweb-2.1-25399 and earlier, where improper input validation in the logon.php script allows an attacker to bypass authentication via SQL injection. Once authenticated as an administrator, the attacker can upload arbitrary PHP code through the importcompany field in import.php, resulting in remote code execution. The malicious payload is injected into /usr/local/astium/web/php/config.php and executed with root privileges by triggering a configuration reload via sudo /sbin/service astcfgd reload. Successful exploitation leads to full	N/A	More Details

	system compromise.		
CVE-2014-125121	Array Networks vAPV (version 8.3.2.17) and vxAG (version 9.2.0.34) appliances are affected by a privilege escalation vulnerability caused by a combination of hardcoded SSH credentials (or SSH private key) and insecure permissions on a startup script. The devices ship with a default SSH login or a hardcoded DSA private key, allowing an attacker to authenticate remotely with limited privileges. Once authenticated, an attacker can overwrite the world-writable /ca/bin/monitor.sh script with arbitrary commands. Since this script is executed with elevated privileges through the backend binary, enabling the debug monitor via backend -c "debug monitor on" triggers execution of the attacker's payload as root. This allows full system compromise.	N/A	More Details
CVE-2014-125122	A stack-based buffer overflow vulnerability exists in the tmUnblock.cgi endpoint of the Linksys WRT120N wireless router. The vulnerability is triggered by sending a specially crafted HTTP POST request with an overly long TM_Block_URL parameter to the endpoint. By exploiting this flaw, an unauthenticated remote attacker can overwrite memory in a controlled manner, enabling them to temporarily reset the administrator password of the device to a blank value. This grants unauthorized access to the router’s web management interface without requiring valid credentials.	N/A	More Details
CVE-2014-125123	An unauthenticated SQL injection vulnerability exists in the Kloxo web hosting control panel (developed by LXCenter) prior to version 6.1.12. The flaw resides in the login-name parameter passed to lbin/webcommand.php, which fails to properly sanitize input, allowing an attacker to extract the administrator’s password from the backend database. After recovering valid credentials, the attacker can authenticate to the Kloxo control panel and leverage the Command Center feature (display.php) to execute arbitrary operating system commands as root on the underlying host system. This vulnerability was reported to be exploited in the wild in January 2014.	N/A	More Details
CVE-2025-53558	ZXHN-F660T and ZXHN-F660A provided by ZTE Japan K.K. use a common credential for all installations. With the knowledge of the credential, an attacker may log in to the affected devices.	N/A	More Details
CVE-2014-125124	An unauthenticated remote command execution vulnerability exists in Pandora FMS versions up to and including 5.0RC1 via the Anyterm web interface, which listens on TCP port 8023. The anyterm-module endpoint accepts unsanitized user input via the p parameter and directly injects it into a shell command, allowing arbitrary command execution as the pandora user. In certain versions (notably 4.1 and 5.0RC1), the pandora user can elevate privileges to root without a password using a chain involving the artica user account. This account is typically installed without a password and is configured to run sudo without authentication. Therefore, full system compromise is possible without any credentials.	N/A	More Details
CVE-2014-125125	A path traversal vulnerability exists in A10 Networks AX Loadbalancer versions 2.6.1-GR1-P5, 2.7.0, and earlier. The vulnerability resides in the handling of the filename parameter in the /xml/downloads endpoint, which fails to properly sanitize user input. An unauthenticated attacker can exploit this flaw by sending crafted HTTP requests containing directory traversal sequences to read arbitrary files outside the intended directory. The files returned by the vulnerable endpoint are deleted from the system after retrieval. This can lead to unauthorized disclosure of sensitive information such as SSL certificates and private keys, as well as unintended file deletion.	N/A	More Details
CVE-2014-125126	An unrestricted file upload vulnerability exists in Simple E-Document versions 3.0 to 3.1 that allows an unauthenticated attacker to bypass authentication by sending a specific cookie header (access=3) with HTTP requests. The application’s upload mechanism fails to restrict file types and does not validate or sanitize user-supplied input, allowing attackers to upload malicious .php scripts. Authentication can be bypassed entirely by supplying a specially crafted cookie (access=3), granting access to the upload functionality without valid credentials. If file uploads are enabled on the server, the attacker can upload a web shell and gain remote code execution with the privileges of the web server user, potentially leading to full system compromise.	N/A	More Details
CVE-2013-10058	An authenticated OS command injection vulnerability exists in various Linksys router models (tested on WRT160Nv2) running firmware version v2.0.03 via the apply.cgi endpoint. The web interface fails to properly sanitize user-supplied input passed to the ping_size parameter during diagnostic operations. An attacker with valid credentials can inject arbitrary shell commands, enabling remote code execution.	N/A	More Details
CVE-2013-10057	A stack-based buffer overflow vulnerability exists in Synactis PDF In-The-Box ActiveX control (PDF_IN_1.ocx), specifically the ConnectToSynactis method. When a long string is passed to this method—intended to populate the ldCmdLine argument of a WinExec call—a strcpy operation overwrites a saved TRegistry class pointer on the stack. This allows remote attackers to execute arbitrary code in the context of the user by enticing them to visit a malicious webpage that instantiates the vulnerable ActiveX control. The vulnerability was discovered via its use in third-party	N/A	More Details

	software such as Logic Print 2013.		
CVE-2013-10055	An unauthenticated arbitrary file upload vulnerability exists in Havalite CMS version 1.1.7 (and possibly earlier) in the upload.php script. The application fails to enforce proper file extension validation and authentication checks, allowing remote attackers to upload malicious PHP files via a crafted multipart/form-data POST request. Once uploaded, the attacker can access the file directly under havalite/tmp/files/, resulting in remote code execution.	N/A	More Details
CVE-2013-10053	A remote command execution vulnerability exists in ZPanel version 10.0.0.2 in its htpasswd module. When creating .htaccess files, the inHTUsername field is passed unsanitized to a system() call that invokes the system's htpasswd binary. By injecting shell metacharacters into the username field, an authenticated attacker can execute arbitrary system commands. Exploitation requires a valid ZPanel account—such as one in the default Users, Resellers, or Administrators groups—but no elevated privileges.	N/A	More Details
CVE-2025-54590	webfinger.js is a TypeScript-based WebFinger client that runs in both browsers and Node.js environments. In versions 2.8.0 and below, the lookup function accepts user addresses for account checking. However, the ActivityPub specification requires preventing access to localhost services in production. This library does not prevent localhost access, only checking for hosts that start with "localhost" and end with a port. Users can exploit this by creating servers that send GET requests with controlled host, path, and port parameters to query services on the instance's host or local network, enabling blind SSRF attacks. This is fixed in version 2.8.1.	N/A	More Details
CVE-2025-4599	The fragment preview functionality in Liferay Portal 7.4.3.61 through 7.4.3.132, and Liferay DXP 2024.Q4.1 through 2024.Q4.5, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.13 and 7.4 update 61 through update 92 was found to be vulnerable to postMessage-based XSS because it allows a remote non-authenticated attacker to inject JavaScript into the fragment portlet URL.	N/A	More Details
CVE-2025-4604	The vulnerable code can bypass the Captcha check in Liferay Portal 7.4.3.80 through 7.4.3.132, and Liferay DXP 2024.Q1.1 through 2024.Q1.19, 2024.Q2.0 through 2024.Q2.13, 2024.Q3.0 through 2024.Q3.13, 2024.Q4.0 through 2024.Q4.7, 2025.Q1.0 through 2025.Q1.15 and 7.4 update 80 through update 92 and then attackers can run scripts in the Gogo shell	N/A	More Details
CVE-2025-53012	MaterialX is an open standard for the exchange of rich material and look-development content across applications and renderers. In version 1.39.2, nested imports of MaterialX files can lead to a crash via stack memory exhaustion, due to the lack of a limit on the "import chain" depth. When parsing file imports, recursion is used to process nested files; however, there is no limit imposed to the depth of files that can be parsed by the library. By building a sufficiently deep chain of MaterialX files one referencing the next, it is possible to crash the process using the MaterialX library via stack exhaustion. This is fixed in version 1.39.3.	N/A	More Details
CVE-2025-7844	Exporting a TPM based RSA key larger than 2048 bits from the TPM could overrun a stack buffer if the default \`MAX_RSA_KEY_BITS=2048\` is used. If your TPM 2.0 module supports RSA key sizes larger than 2048 bit and your applications supports creating or importing an RSA private or public key larger than 2048 bits and your application calls \`wolfTPM2_RsaKey_TpmToWolf\` on that key, then a stack buffer could be overrun. If the \`MAX_RSA_KEY_BITS\` build-time macro is set correctly (RSA bits match what TPM hardware is capable of) for the hardware target, then a stack overrun is not possible.	N/A	More Details
CVE-2025-1394	Failure to handle the error status returned by the buffer management APIs in SiLabs EmberZNet Zigbee stack may result in data leaks or potential Denial of Service (DoS).	N/A	More Details
CVE-2025-1221	A Zigbee Radio Co-Processor (RCP), which is using SiLabs EmberZNet Zigbee stack, was unable to send messages to the host system (CPCd) due to heavy Zigbee traffic, resulting in a Denial of Service (DoS) attack, Only hard reset will bring the device to normal operation	N/A	More Details
CVE-2012-10021	A stack-based buffer overflow vulnerability exists in D-Link DIR-605L Wireless N300 Cloud Router firmware versions 1.12 and 1.13 via the getAuthCode() function. The flaw arises from unsafe usage of sprintf() when processing user-supplied CAPTCHA data via the FILECODE parameter in /goform/formLogin. A remote unauthenticated attacker can exploit this to execute arbitrary code with root privileges on the device.	N/A	More Details
CVE-2025-38498	In the Linux kernel, the following vulnerability has been resolved: do_change_type(): refuse to operate on unmounted/not ours mounts Ensure that propagation settings can only be changed for mounts located in the caller's mount namespace. This change aligns permission checking with the	N/A	More Details

	rest of mount(2).		
CVE-2025-53011	MaterialX is an open standard for the exchange of rich material and look-development content across applications and renderers. In version 1.39.2, when parsing shader nodes in a MTLX file, the MaterialXCore code accesses a potentially null pointer, which can lead to crashes with maliciously crafted files. An attacker could intentionally crash a target program that uses MaterialX by sending a malicious MTLX file. This is fixed in version 1.39.3.	N/A	More Details
CVE-2025-54797	Rejected reason: This CVE is a duplicate of CVE-2025-52464.	N/A	More Details
CVE-2025-53010	MaterialX is an open standard for the exchange of rich material and look-development content across applications and renderers. In version 1.39.2, when parsing shader nodes in a MTLX file, the MaterialXCore code accesses a potentially null pointer, which can lead to crashes with maliciously crafted files. An attacker could intentionally crash a target program that uses OpenEXR by sending a malicious MTLX file. This is fixed in version 1.39.3.	N/A	More Details
CVE-2025-8321	Tesla Wall Connector Firmware Downgrade Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Tesla Wall Connector devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the firmware upgrade feature. The issue results from the lack of an anti-downgrade mechanism. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the device. Was ZDI-CAN-26299.	N/A	More Details
CVE-2025-8320	Tesla Wall Connector Content-Length Header Improper Input Validation Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Tesla Wall Connector devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of the HTTP Content-Length header. The issue results from the lack of proper validation of user-supplied data, which can result in memory access past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-26300.	N/A	More Details
CVE-2025-54387	IPX is an image optimizer powered by sharp and svgo. In versions 1.3.1 and below, 2.0.0-0 through 2.1.0, and 3.0.0 through 3.1.0, the approach used to check whether a path is within allowed directories is vulnerable to path prefix bypass when the allowed directories do not end with a path separator. This occurs because the check relies on a raw string prefix comparison. This is fixed in versions 1.3.2, 2.1.1 and 3.1.1.	N/A	More Details
CVE-2025-53009	MaterialX is an open standard for the exchange of rich material and look-development content across applications and renderers. In versions 1.39.2 and below, when parsing an MTLX file with multiple nested nodegraph implementations, the MaterialX XML parsing logic can potentially crash due to stack exhaustion. An attacker could intentionally crash a target program that uses OpenEXR by sending a malicious MTLX file. This is fixed in version 1.39.3.	N/A	More Details
CVE-2025-54794	Claude Code is an agentic coding tool. In versions below 0.2.111, a path validation flaw using prefix matching instead of canonical path comparison, makes it possible to bypass directory restrictions and access files outside the CWD. Successful exploitation depends on the presence of (or ability to create) a directory with the same prefix as the CWD and the ability to add untrusted content into a Claude Code context window. This is fixed in version 0.2.111.	N/A	More Details
CVE-2025-54795	Claude Code is an agentic coding tool. In versions below 1.0.20, an error in command parsing makes it possible to bypass the Claude Code confirmation prompt to trigger execution of an untrusted command. Reliably exploiting this requires the ability to add untrusted content into a Claude Code context window. This is fixed in version 1.0.20.	N/A	More Details
CVE-2025-54803	js-toml is a TOML parser for JavaScript, fully compliant with the TOML 1.0.0 Spec. In versions below 1.0.2, a prototype pollution vulnerability in js-toml allows a remote attacker to add or modify properties of the global Object.prototype by parsing a maliciously crafted TOML input. This is fixed in version 1.0.2.	N/A	More Details
CVE-2025-8472	Alpine iLX-507 vCard Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-507 devices. User interaction is required to exploit this vulnerability in that the target must connect to a malicious Bluetooth device. The specific flaw exists within the parsing of vCard data. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute arbitrary code in the context of root. Was ZDI-CAN-26316.	N/A	More Details

CVE-2025-8473	Alpine iLX-507 UPDM_wstpCBCUpdStart Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine iLX-507 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPDM_wstpCBCUpdStart function. The issue results from the lack of proper validation of user-supplied data before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-26317.	N/A	More Details
CVE-2025-54388	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker Engine, Mirantis Container Runtime, and various other downstream projects/products. In versions 28.2.0 through 28.3.2, when the firewalld service is reloaded it removes all iptables rules including those created by Docker. While Docker should automatically recreate these rules, versions before 28.3.3 fail to recreate the specific rules that block external access to containers. This means that after a firewalld reload, containers with ports published to localhost (like 127.0.0.1:8080) become accessible from remote machines that have network routing to the Docker bridge, even though they should only be accessible from the host itself. The vulnerability only affects explicitly published ports - unpublished ports remain protected. This issue is fixed in version 28.3.3.	N/A	More Details
CVE-2012-10022	Kloxo versions 6.1.12 and earlier contain two setuid root binaries—lxsuexec and lxrestart—that allow local privilege escalation from uid 48. The lxsuexec binary performs a uid check and permits execution of arbitrary commands as root if the invoking user matches uid 48. This flaw enables attackers with Apache-level access to escalate privileges to root without authentication.	N/A	More Details
CVE-2013-10051	A remote PHP code execution vulnerability exists in InstantCMS version 1.6 and earlier due to unsafe use of eval() within the search view handler. Specifically, user-supplied input passed via the look parameter is concatenated into a PHP expression and executed without proper sanitation. A remote attacker can exploit this flaw by sending a crafted HTTP GET request with a base64-encoded payload in the Cmd header, resulting in arbitrary PHP code execution within the context of the web server.	N/A	More Details
CVE-2013-10050	An OS command injection vulnerability exists in multiple D-Link routers—confirmed on DIR-300 rev A (v1.05) and DIR-615 rev D (v4.13)—via the authenticated tools_vct.xgi CGI endpoint. The web interface fails to properly sanitize user-supplied input in the pingIp parameter, allowing attackers with valid credentials to inject arbitrary shell commands. Exploitation enables full device compromise, including spawning a telnet daemon and establishing a root shell. The vulnerability is present in firmware versions that expose tools_vct.xgi and use the Mathopd/1.5p6 web server. No vendor patch is available, and affected models are end-of-life.	N/A	More Details
CVE-2013-10049	An OS command injection vulnerability exists in multiple Raidsonic NAS devices—specifically tested on IB-NAS5220 and IB-NAS4220—via the unauthenticated timeHandler.cgi endpoint exposed through the web interface. The CGI script fails to properly sanitize user-supplied input in the timeZone parameter of a POST request, allowing remote attackers to inject arbitrary shell commands.	N/A	More Details
CVE-2013-10048	An OS command injection vulnerability exists in various legacy D-Link routers—including DIR-300 rev B and DIR-600 (firmware ≤ 2.13 and ≤ 2.14b01, respectively)—due to improper input handling in the unauthenticated command.php endpoint. By sending specially crafted POST requests, a remote attacker can execute arbitrary shell commands with root privileges, allowing full takeover of the device. This includes launching services such as Telnet, exfiltrating credentials, modifying system configuration, and disrupting availability. The flaw stems from the lack of authentication and inadequate sanitation of the cmd parameter.	N/A	More Details
CVE-2025-54433	Bugsink is a self-hosted error tracking service. In versions 1.4.2 and below, 1.5.0 through 1.5.4, 1.6.0 through 1.6.3, and 1.7.0 through 1.7.3, ingestion paths construct file locations directly from untrusted event_id input without validation. A specially crafted event_id can result in paths outside the intended directory, potentially allowing file overwrite or creation in arbitrary locations. Submitting such input requires access to a valid DSN, potentially exposing them. If Bugsink runs in a container, the effect is confined to the container's filesystem. In non-containerized setups, the overwrite may affect other parts of the system accessible to that user. This is fixed in versions 1.4.3, 1.5.5, 1.6.4 and 1.7.4.	N/A	More Details
CVE-2013-10047	An unrestricted file upload vulnerability exists in MiniWeb HTTP Server <= Build 300 that allows unauthenticated remote attackers to upload arbitrary files to the server's filesystem. By abusing the upload handler and crafting a traversal path, an attacker can place a malicious .exe in system32, followed by a .mof file in the WMI directory. This triggers execution of the payload with SYSTEM privileges via the Windows Management Instrumentation service. The exploit is only viable on Windows versions prior to Vista.	N/A	More Details
	A local privilege escalation vulnerability exists in Agnitum Outpost Internet Security 8.1 that allows an unprivileged user to execute arbitrary code with SYSTEM privileges. The flaw resides in the		

CVE-2013-10046	acs.exe component, which exposes a named pipe that accepts unauthenticated commands. By exploiting a directory traversal weakness in the pipe protocol, an attacker can instruct the service to load a malicious DLL from a user-controlled location. The DLL is then executed in the context of the privileged service.	N/A	More Details
CVE-2013-10044	An authenticated SQL injection vulnerability exists in OpenEMR ≤ 4.1.1 Patch 14 that allows a low-privileged attacker to extract administrator credentials and subsequently escalate privileges. Once elevated, the attacker can exploit an unrestricted file upload flaw to achieve remote code execution, resulting in full compromise of the application and its host system.	N/A	More Details
CVE-2025-8480	Alpine iLX-507 Command Injection Remote Code Execution. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-507 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Tidal music streaming application. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-26357.	N/A	More Details
CVE-2025-8474	Alpine iLX-507 CarPlay Stack-based Buffer Overflow Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine iLX-507 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the Apple CarPlay protocol. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-26318.	N/A	More Details
CVE-2025-8477	Alpine iLX-507 vCard Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected Alpine iLX-507 devices. User interaction is required to exploit this vulnerability in that the target must connect to a malicious Bluetooth device. The specific flaw exists within the parsing of vCard data. The issue results from the lack of proper validation of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-26324.	N/A	More Details
CVE-2013-10052	ZPanel includes a helper binary named zsudo, intended to allow restricted privilege escalation for administrative tasks. However, when misconfigured in /etc/sudoers, zsudo can be invoked by low-privileged users to execute arbitrary commands as root. This flaw enables local attackers with shell access to escalate privileges by writing a payload to a writable directory and executing it via zsudo. The vulnerability is particularly impactful in post-exploitation scenarios following web server compromise, where the attacker inherits access to zsudo.	N/A	More Details
CVE-2013-10054	An unauthenticated arbitrary file upload vulnerability exists in LibrettoCMS version 1.1.7 (and possibly earlier) contains an unauthenticated arbitrary file upload vulnerability in its File Manager plugin. The upload handler located at adm/ui/js/ckeditor/plugins/pgrfilemanager/php/upload.php fails to properly validate file extensions, allowing attackers to upload files with misleading extensions and subsequently rename them to executable .php scripts. This enables remote code execution on the server without authentication.	N/A	More Details
CVE-2025-43018	Certain HP LaserJet Pro printers may be vulnerable to information disclosure when a non-authenticated user queries a device’s local address book.	N/A	More Details
CVE-2025-34147	An unauthenticated OS command injection vulnerability exists in the Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02). When configuring the device in Extender mode via its captive portal, the extap2g SSID field is inserted unescaped into a reboot-time shell script. This allows remote attackers within Wi-Fi range to inject arbitrary shell commands that execute as root during device reboot, leading to full system compromise.	N/A	More Details
CVE-2025-8476	Alpine iLX-507 TIDAL Improper Certificate Validation Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-507 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the TIDAL music streaming application. The issue results from improper certificate validation. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-26322.	N/A	More Details
CVE-	Alpine iLX-507 AVRCP Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-507 devices. User interaction is required to exploit this vulnerability in that the target		More

2025-8475	must connect to a malicious Bluetooth device. The specific flaw exists within the implementation of the AVRCP protocol. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-26321.	N/A	Details
CVE-2025-54572	The Ruby SAML library is for implementing the client side of a SAML authorization. In versions 1.18.0 and below, a denial-of-service vulnerability exists in ruby-saml even with the message_max_bytesize setting configured. The vulnerability occurs because the SAML response is validated for Base64 format prior to checking the message size, leading to potential resource exhaustion. This is fixed in version 1.18.1.	N/A	More Details
CVE-2025-8573	Concrete CMS versions 9 through 9.4.2 are vulnerable to Stored XSS from Home Folder on Members Dashboard page. Version 8 was not affected. A rogue admin could set up a malicious folder containing XSS to which users could be directed upon login. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 2.0 with vector CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N. Thanks sealldev for reporting via HackerOne.	N/A	More Details