SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 December 2025

Generated on 03 December 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-2025-63531	A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the receiverLogin.php component. The application fails to properly sanitize user-supplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the remail and rpassword fields, an attacker can bypass authentication and gain unauthorized access to the system.	10.0	More Details
CVE-2025-64126	An OS command injection vulnerability exists due to improper input validation. The application accepts a parameter directly from user input without verifying it is a valid IP address or filtering potentially malicious characters. This could allow an unauthenticated attacker to inject arbitrary commands.	10.0	More Details
CVE-2025-64127	An OS command injection vulnerability exists due to insufficient sanitization of user-supplied input. The application accepts parameters that are later incorporated into OS commands without adequate validation. This could allow an unauthenticated attacker to execute arbitrary commands remotely.	10.0	More Details
CVE-2025-64128	An OS command injection vulnerability exists due to incomplete validation of user-supplied input. Validation fails to enforce sufficient formatting rules, which could permit attackers to append arbitrary data. This could allow an unauthenticated attacker to inject arbitrary commands.	10.0	More Details
CVE-2025-12421	Mattermost versions 11.0.x <= 11.0.2, 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12 fail to to verify that the token used during the code exchange originates from the same authentication flow, which allows an authenticated user to perform account takeover via a specially crafted email address used when switching authentication methods and sending a request to the /users/login/sso/code-exchange endpoint. The vulnerability requires ExperimentalEnableAuthenticationTransfer to be enabled (default: enabled) and RequireEmailVerification to be disabled (default: disabled).	9.9	More Details
	Mattermost versions 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12, 11.0.x <=		

CVE-2025-12419	11.0.3 fail to properly validate OAuth state tokens during OpenID Connect authentication which allows an authenticated attacker with team creation privileges to take over a user account via manipulation of authentication data during the OAuth completion flow. This requires email verification to be disabled (default: disabled), OAuth/OpenID Connect to be enabled, and the attacker to control two users in the SSO system with one of them never having logged into Mattermost.	9.9	More Details
CVE-2025-13675	The Tiger theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 101.2.1. This is due to the 'paypal-submit.php' file not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2025-13538	The FindAll Listing plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.5. This is due to the 'findall_listing_user_registration_additional_params' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site. Note: The vulnerability can only be exploited if the FindAll Membership plugin is also activated, because user registration is in that plugin.	9.8	More Details
CVE-2025-41742	Sprecher Automations SPRECON-E-C, SPRECON-E-P, SPRECON-E-T3 is vulnerable to attack by an unauthorized remote attacker via default cryptographic keys. The use of these keys allows the attacker to read, modify, and write projects and data, or to access any device via remote maintenance.	9.8	More Details
CVE-2025-66401	MCP Watch is a comprehensive security scanner for Model Context Protocol (MCP) servers. In 0.1.2 and earlier, the MCPScanner class contains a critical Command Injection vulnerability in the cloneRepo method. The application passes the user-supplied githubUrl argument directly to a system shell via execSync without sanitization. This allows an attacker to execute arbitrary commands on the host machine by appending shell metacharacters to the URL.	9.8	More Details
CVE-2025-51682	mJobtime 15.7.2 handles authorization on the client side, which allows an attacker to modify the client-side code and gain access to administrative features. Additionally, they can craft requests based on the client-side code to call these administrative functions directly.	9.8	More Details
CVE-2025-13615	The StreamTube Core plugin for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 4.78. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts. Note: This can only be exploited if the 'registration password fields' enabled in theme options.	9.8	More Details
CVE-2025-64657	Stack-based buffer overflow in Azure Application Gateway allows an unauthorized attacker to elevate privileges over a network.	9.8	More Details
CVE-2025-13540	The Tiare Membership plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2. This is due to the 'tiare_membership_init_rest_api_register' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2025-13539	The FindAll Membership plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.4. This is due to the plugin not properly logging in a user with the data that was previously verified through the 'findall_membership_check_facebook_user' and the 'findall_membership_check_google_user' functions. This makes it possible for unauthenticated attackers to log in as administrative users, as long as they have an existing account on the site which can easily be created by default through the temp user functionality, and access to the administrative user's email.	9.8	More Details
CVE-2025-13542	The DesignThemes LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.4. This is due to the 'dtlms_register_user_front_end' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.	9.8	More Details
CVE-2025-65236	OpenCode Systems USSD Gateway OC Release: 5 was discovered to contain a SQL injection vulnerability via the Session ID parameter in the /occontrolpanel/index.php endpoint.	9.8	More Details

CVE-2025-50433	An issue was discovered in imonnit.com (2025-04-24) allowing malicious actors to gain escalated privileges via crafted password reset to take over arbitrary user accounts.	9.8	More Details
CVE-2025-26155	NCP Secure Enterprise Client 13.18 and NCP Secure Entry Windows Client 13.19 have an Untrusted Search Path vulnerability.	9.8	More Details
CVE-2025-64130	Zenitel TCIV-3+ is vulnerable to a reflected cross-site scripting vulnerability, which could allow a remote attacker to execute arbitrary JavaScript on the victim's browser.	9.8	More Details
CVE-2025-59390	Apache Druid’s Kerberos authenticator uses a weak fallback secret when the `druid.auth.authenticator.kerberos.cookieSignatureSecret` configuration is not explicitly set. In this case, the secret is generated using `ThreadLocalRandom`, which is not a crypto-graphically secure random number generator. This may allow an attacker to predict or brute force the secret used to sign authentication cookies, potentially enabling token forgery or authentication bypass. Additionally, each process generates its own fallback secret, resulting in inconsistent secrets across nodes. This causes authentication failures in distributed or multi-broker deployments, effectively leading to a incorrectly configured clusters. Users are advised to configure a strong `druid.auth.authenticator.kerberos.cookieSignatureSecret` This issue affects Apache Druid: through 34.0.0. Users are recommended to upgrade to version 35.0.0, which fixes the issue making it mandatory to set `druid.auth.authenticator.kerberos.cookieSignatureSecret` when using the Kerberos authenticator. Services will fail to come up if the secret is not set.	9.8	More Details
CVE-2025-62354	Improper neutralization of special elements used in an OS command ('command injection') in Cursor allows an unauthorized attacker to execute commands that are outside of those specified in the allowlist, resulting in arbitrary code execution.	9.8	More Details
CVE-2025-55469	Incorrect access control in youlai-boot v2.21.1 allows attackers to escalate privileges and access the Administrator backend.	9.8	More Details
CVE-2025-65276	An unauthenticated administrative access vulnerability exists in the open-source HashTech project (https://github.com/henzljw/hashtech) 1.0 thru commit 5919decaff2681dc250e934814fc3a35f6093ee5 (2021-07-02). Due to missing authentication checks on /admin_index.php, an attacker can directly access the admin dashboard without valid credentials. This allows full administrative control including viewing/modifying user accounts, managing orders, changing payments, and editing product listings. Successful exploitation can lead to information disclosure, data manipulation, and privilege escalation.	9.8	More Details
CVE-2025-63525	An issue was discovered in Blood Bank Management System 1.0 allowing authenticated attackers to perform actions with escalated privileges via crafted request to delete.php.	9.6	More Details
CVE-2025-66022	FACTION is a PenTesting Report Generation and Collaboration Framework. Prior to version 1.7.1, an extension execution path in Faction’s extension framework permits untrusted extension code to execute arbitrary system commands on the server when a lifecycle hook is invoked, resulting in remote code execution (RCE) on the host running Faction. Due to a missing authentication check on the /portal/AppStoreDashboard endpoint, an attacker can access the extension management UI and upload a malicious extension without any authentication, making this vulnerability exploitable by unauthenticated users. This issue has been patched in version 1.7.1.	9.6	More Details
CVE-2025-63535	A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the abs.php component. The application fails to properly sanitize usersupplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the search field, an attacker can bypass authentication and gain unauthorized access to the system.	9.6	More Details
CVE-2025-63532	A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the cancel.php component. The application fails to properly sanitize user-supplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the search field, an attacker can bypass authentication and gain unauthorized access to the system.	9.6	More Details
CVE-2025-64656	Out-of-bounds read in Application Gateway allows an unauthorized attacker to elevate privileges over a network.	9.4	More Details
CVE-2025-65112	PubNet is a self-hosted Dart & Flutter package service. Prior to version 1.1.3, the /api/storage/upload endpoint in PubNet allows unauthenticated users to upload packages as any user by providing arbitrary author-id values. This enables identity spoofing, privilege	9.4	More Details

	escalation, and supply chain attacks. This issue has been patched in version 1.1.3.		
CVE-2025-64314	Permission control vulnerability in the memory management module. Impact: Successful exploitation of this vulnerability may affect confidentiality.	9.3	More Details
CVE-2025-40934	XML-Sig versions 0.27 through 0.67 for Perl incorrectly validates XML files if signatures are omitted. An attacker can remove the signature from the XML document to make it pass the verification check. XML-Sig is a Perl module to validate signatures on XML files. An unsigned XML file should return an error message. The affected versions return true when attempting to validate an XML file that contains no signatures.	9.3	More Details
CVE-2025-12106	Insufficient argument validation in OpenVPN 2.7_alpha1 through 2.7_rc1 allows an attacker to trigger a heap buffer over-read when parsing IP addresses	9.1	More Details
CVE-2025-35028	By providing a command-line argument starting with a semi-colon ; to an API endpoint created by the EnhancedCommandExecutor class of the HexStrike AI MCP server, the resultant composed command is executed directly in the context of the MCP server's normal privilege; typically, this is root. There is no attempt to sanitize these arguments in the default configuration of this MCP server at the affected version (as of commit 2f3a5512 in September of 2025).	9.1	More Details
CVE-2025-65836	PublicCMS V5.202506.b is vulnerable to SSRF. in the chat interface of SimpleAiAdminController.	9.1	More Details
CVE-2025-65669	An issue was discovered in classroomio 0.1.13. Student accounts are able to delete courses from the Explore page without any authorization or authentication checks, bypassing the expected admin-only deletion restriction.	9.1	More Details
CVE-2025-41744	Sprecher Automations SPRECON-E series uses default cryptographic keys that allow an unprivileged remote attacker to access all encrypted communications, thereby compromising confidentiality and integrity.	9.1	More Details
CVE-2025-3500	Integer Overflow or Wraparound vulnerability in Avast Antivirus (25.1.981.6) on Windows allows Privilege Escalation.This issue affects Antivirus: from 25.1.981.6 before 25.3.	9.0	More Details
CVE-2025-8351	Heap-based Buffer Overflow, Out-of-bounds Read vulnerability in Avast Antivirus on MacOS when scanning a malformed file may allow Local Execution of Code or Denial-of-Service of the anitvirus engine process.This issue affects Antivirus: from 8.3.70.94 before 8.3.70.98.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-13720	Bad cast in Loader in Google Chrome prior to 143.0.7499.41 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2025-13638	Use after free in Media Stream in Google Chrome prior to 143.0.7499.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2025-65840	PublicCMS V5.202506.b is vulnerable to Cross Site Request Forgery (CSRF) in the CkEditorAdminController.	8.8	More Details
CVE-2025-13536	The Blubrry PowerPress plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in all versions up to, and including, 11.15.2. This is due to the plugin validating file extensions but not halting execution when validation fails in the 'powerpress_edit_post' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, Grav CMS is vulnerable to a Server-Side Template Injection (SSTI) that allows any authenticated user with editor permissions to execute arbitrary code on the remote server, bypassing the existing security sandbox. Since the security		

CVE-2025-66299	sandbox does not fully protect the Twig object, it is possible to interact with it (e.g., call methods, read/write attributes) through maliciously crafted Twig template directives injected into a web page. This allows an authenticated editor to add arbitrary functions to the Twig attribute system.twig.safe_filters, effectively bypassing the Grav CMS sandbox. This vulnerability is fixed in 1.8.0-beta.27.	8.8	More Details
CVE-2025-13680	The Tiger theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 101.2.1. This is due to the plugin allowing a user to update the user role through the $user->set_role() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to that of an administrator.	8.8	More Details
CVE-2025-45311	Insecure permissions in fail2ban-client v0.11.2 allows attackers with limited sudo privileges to perform arbitrary operations as root. NOTE: this is disputed by multiple parties because the action for a triggered rule can legitimately be an arbitrary operation as root. Thus, the software is behaving in accordance with its intended privilege model.	8.8	More Details
CVE-2025-13630	Type Confusion in V8 in Google Chrome prior to 143.0.7499.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-13631	Inappropriate implementation in Google Updater in Google Chrome on Mac prior to 143.0.7499.41 allowed a remote attacker to perform privilege escalation via a crafted file. (Chromium security severity: High)	8.8	More Details
CVE-2025-13633	Use after free in Digital Credentials in Google Chrome prior to 143.0.7499.41 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-12529	The Cost Calculator Builder plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the deleteOrdersFiles() function in all versions up to, and including, 3.6.3. This makes it possible for unauthenticated attackers to inject arbitrary file paths into the orders that are removed, when an administrator deletes them. This can lead to remote code execution when the right file is deleted (such as wp-config.php). This vulnerability requires the Cost Calculator Builder Pro version to be installed along with the free version in order to be exploitable.	8.8	More Details
CVE-2025-66296	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, a privilege escalation vulnerability exists in Grav's Admin plugin due to the absence of username uniqueness validation when creating users. A user with the create user permission can create a new account using the same username as an existing administrator account, set a new password/email, and then log in as that administrator. This effectively allows privilege escalation from limited user-manager permissions to full administrator access. This vulnerability is fixed in 1.8.0-beta.27.	8.8	More Details
CVE-2025-13757	SQL Injection vulnerability in last usage logs in Devolutions Server.This issue affects Devolutions Server: through 2025.2.20, through 2025.3.8.	8.8	More Details
CVE-2025-66295	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, when a user with privilege of user creation creates a new user through the Admin UI and supplies a username containing path traversal sequences (for example ..\Nijat or ../Nijat), Grav writes the account YAML file to an unintended path outside user/accounts/. The written YAML can contain account fields such as email, fullname, twofa_secret, and hashed_password. This vulnerability is fixed in 1.8.0-beta.27.	8.8	More Details
CVE-2025-12061	The TAX SERVICE Electronic HDM WordPress plugin before 1.2.1 does not authorization and CSRF checks in an AJAX action, allowing unauthenticated users to import and execute arbitrary SQL statements	8.6	More Details
CVE-2024-48882	A denial of service vulnerability exists in the Modbus TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to denial of service. An attacker can send an unauthenticated packet to trigger this vulnerability.	8.6	More Details
CVE-2025-55221	A denial of service vulnerability exists in the Modbus TCP and Modbus RTU over TCP USB Function functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to a denial of service. An attacker can send an unauthenticated packet to trigger this vulnerability.This vulnerability is specific to the malicious message sent via Modbus TCP over port 502.	8.6	More Details

CVE-2025-55222	A denial of service vulnerability exists in the Modbus TCP and Modbus RTU over TCP USB Function functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to a denial of service. An attacker can send an unauthenticated packet to trigger this vulnerability.This vulnerability is specific to the malicious message sent via Modbus RTU over TCP on port 503.	8.6	More Details
CVE-2025-23417	A denial of service vulnerability exists in the Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to denial of service. An attacker can send an unauthenticated packet to trigger this vulnerability.	8.6	More Details
CVE-2025-26858	A buffer overflow vulnerability exists in the Modbus TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted set of network packets can lead to denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.	8.6	More Details
CVE-2025-66359	An issue was discovered in Logpoint before 7.7.0. Insufficient input validation and a lack of output escaping in multiple components leads to a cross-site scripting (XSS) vulnerability.	8.5	More Details
CVE-2025-63528	A cross-site scripting (XSS) vulnerability exists in the Blood Bank Management System 1.0 within the blooddinfo.php component. The application fails to properly sanitize or encode user-supplied input before rendering it in response. An attacker can inject malicious JavaScript payloads into the error parameter, which is then executed in the victim's browser when the page is viewed.	8.5	More Details
CVE-2025-63534	A cross-site scripting (XSS) vulnerability exists in the Blood Bank Management System 1.0 within the login.php component. The application fails to properly sanitize or encode user-supplied input before rendering it in response. An attacker can inject malicious JavaScript payloads into the msg and error parameters, which are then executed in the victim's browser when the page is viewed.	8.5	More Details
CVE-2025-63533	A cross-site scripting (XSS) vulnerability exists in the Blood Bank Management System 1.0 within the updateprofile.php and rprofile.php components. The application fails to properly sanitize or encode user-supplied input before rendering it in response. An attacker can inject malicious JavaScript payloads into the rname, remail, rpassword, rphone, rcity parameters, which are then executed in the victim's browser when the page is viewed.	8.5	More Details
CVE-2025-63527	A cross-site scripting (XSS) vulnerability exists in the Blood Bank Management System 1.0 within the updateprofile.php and hprofile.php components. The application fails to properly sanitize or encode user-supplied input before rendering it in response. An attacker can inject malicious JavaScript payloads into the hname, hemail, hpassword, hphone, hcity parameters, which are then executed in the victim's browser when the page is viewed.	8.5	More Details
CVE-2025-63526	A cross-site scripting (XSS) vulnerability exists in the Blood Bank Management System within the abs.php component. The application fails to properly sanitize or encode user-supplied input before rendering it in response. An attacker can inject malicious JavaScript payloads into the msg parameter, which is then executed in the victim's browser when the page is viewed.	8.5	More Details
CVE-2025-66300	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, A low privilege user account with page editing privilege can read any server files using "Frontmatter" form. This includes Grav user account files (/grav/user/accounts/*.yaml), which store hashed user password, 2FA secret, and the password reset token. This can allow an adversary to compromise any registered account by resetting a password for a user to get access to the password reset token from the file or by cracking the hashed password. This vulnerability is fixed in 1.8.0-beta.27.	8.5	More Details
CVE-2025-58303	UAF vulnerability in the screen recording framework module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2025-64298	NMIS/BioDose V22.02 and previous version installations where the embedded Microsoft SQLServer Express is used are exposed in the Windows share accessed by clients in networked installs. By default, this directory has insecure directory paths that allow access to the SQL Server database and configuration files, which can contain sensitive data.	8.4	More Details
CVE-2024-45675	IBM Informix Dynamic Server 14.10 could allow a local user on the system to log into the Informix server as administrator without a password.	8.4	More Details
CVE-			

2025-58302	Permission control vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	8.4	More Details
CVE-2025-61940	NMIS/BioDose V22.02 and previous versions rely on a common SQL Server user account to access data in the database. User access in the client application is restricted by a password authentication check in the client software but the underlying database connection always has access. The latest version of NMIS/BioDose introduces an option to use Windows user authentication with the database, which would restrict this database connection.	8.3	More Details
CVE-2025-62575	NMIS/BioDose V22.02 and previous versions rely on a Microsoft SQL Server database. The SQL user account 'nmdbuser' and other created accounts by default have the sysadmin role. This can lead to remote code execution through the use of certain built-in stored procedures.	8.3	More Details
CVE-2025-66384	app/Controller/EventsController.php in MISP before 2.5.24 has invalid logic in checking for uploaded file validity, related to tmp_name.	8.2	More Details
CVE-2025-57489	Incorrect access control in the SDAgent component of Shirt Pocket SuperDuper! v3.10 allows attackers to escalate privileges to root due to the improper use of a setuid binary.	8.1	More Details
CVE-2025-13516	The SureMail – SMTP and Email Logs Plugin for WordPress is vulnerable to Unrestricted Upload of File with Dangerous Type in versions up to and including 1.9.0. This is due to the plugin's save_file() function in inc/emails/handler/uploads.php which duplicates all email attachments to a web-accessible directory (wp-content/uploads/suremails/attachments/) without validating file extensions or content types. Files are saved with predictable names derived from MD5 hashes of their content. While the plugin attempts to protect this directory with an Apache .htaccess file to disable PHP execution, this protection is ineffective on nginx, IIS, and Lighttpd servers, or on misconfigured Apache installations. This makes it possible for unauthenticated attackers to achieve Remote Code Execution by uploading malicious PHP files through any public form that emails attachments, calculating the predictable filename, and directly accessing the file to execute arbitrary code granted they are exploiting a site running on an affected web server configuration.	8.1	More Details
CVE-2025-10101	Heap-based Buffer Overflow, Out-of-bounds Write vulnerability in Avast Antivirus on MacOS of a crafted Mach-O file may allow Local Execution of Code or Denial of Service of antivirus protection. This issue affects Antivirus: from 15.7 before 3.9.2025.	8.1	More Details
CVE-2024-39148	The service wmp-agent of KerOS prior 5.12 does not properly validate so-called ‘magic URLs’ allowing an unauthenticated remote attacker to execute arbitrary OS commands as root when the service is reachable over network. Typically, the service is protected via local firewall.	8.1	More Details
CVE-2025-58310	Permission control vulnerability in the distributed component. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	8.0	More Details
CVE-2025-64642	NMIS/BioDose V22.02 and previous versions' installation directory paths by default have insecure file permissions, which in certain deployment scenarios can enable users on client workstations to modify the program executables and libraries.	8.0	More Details
CVE-2025-65202	TRENDnet TEW-657BRM 1.00.1 has an authenticated remote OS command injection vulnerability in the setup.cgi binary, exploitable via the HTTP parameters "command", "todo", and "next_file," which allows an attacker to execute arbitrary commands with root privileges.	8.0	More Details
CVE-2025-20767	In display, there is a possible out of bounds write due to an integer overflow. 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: ALPS10196993; Issue ID: MSV-4807.	7.8	More Details
CVE-2025-20768	In display, there is a possible out of bounds read 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: ALPS10196993; Issue ID: MSV-4805.	7.8	More Details
CVE-2025-	Vim is an open source, command line text editor. Prior to version 9.1.1947, an uncontrolled search path vulnerability on Windows allows Vim to execute malicious executables placed in the current working directory for the current edited file. On Windows, when using cmd.exe as a shell, Vim resolves external commands by searching the current working directory before system	7.8	More

66476	paths. When Vim invokes tools such as findstr for :grep, external commands or filters via :!, or compiler/:make commands, it may inadvertently run a malicious executable present in the same directory as the file being edited. The issue affects Vim for Windows prior to version 9.1.1947.		Details
CVE-2025-20763	In mmdvfs, 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: ALPS10267218; Issue ID: MSV-5032.	7.8	More Details
CVE-2025-20764	In smi, 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: ALPS10259774; Issue ID: MSV-5029.	7.8	More Details
CVE-2025-20766	In display, there is a possible memory corruption due to improper input validation. 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: ALPS10196993; Issue ID: MSV-4820.	7.8	More Details
CVE-2025-41700	An unauthenticated attacker can trick a local user into executing arbitrary code by opening a deliberately manipulated CODESYS project file with a CODESYS development system. This arbitrary code is executed in the user context.	7.8	More Details
CVE-2025-61228	An issue in Shirt Pocket SuperDuper! V.3.10 and before allows a local attacker to execute arbitrary code via the software update mechanism	7.8	More Details
CVE-2025-13000	The db-access WordPress plugin through 0.8.7 does not have authorization in an AJAX action, allowing any authenticated users, such as subscriber to perform SQLI attacks	7.7	More Details
CVE-2025-13601	A heap-based buffer overflow problem was found in glib through an incorrect calculation of buffer size in the g_escape_uri_string() function. If the string to escape contains a very large number of unacceptable characters (which would need escaping), the calculation of the length of the escaped string could overflow, leading to a potential write off the end of the newly allocated string.	7.7	More Details
CVE-2025-66468	The Aimeos GrapesJS CMS extension provides page editor for creating content pages based on extensible components. Prior to 2021.10.8, 2022.10.8, 2023.10.8, 2024.10.8, and 2025.10.8, Javascript code can be injected by malicious editors for a stored XSS attack if the standard Content Security Policy is disabled. This vulnerability is fixed in 2021.10.8, 2022.10.8, 2023.10.8, 2024.10.8, and 2025.10.8.	7.6	More Details
CVE-2025-9558	There is a potential OOB Write vulnerability in the gen_prov_start function in pb_adv.c. The full length of the received data is copied into the link.rx.buf receiver buffer without any validation on the data size.	7.6	More Details
CVE-2025-9557	An out-of-bound write can lead to an arbitrary code execution. Even on devices with some form of memory protection, this can still lead to a crash and a resultant denial of service.	7.6	More Details
CVE-2025-13084	The users endpoint in the groov View API returns a list of all users and associated metadata including their API keys. This endpoint requires an Editor role to access and will display API keys for all users, including Administrators.	7.6	More Details
CVE-2025-64129	Zenitel TCIV-3+ is vulnerable to an out-of-bounds write vulnerability, which could allow a remote attacker to crash the device.	7.6	More Details
CVE-2025-64334	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. In versions from 8.0.0 to before 8.0.2, compressed HTTP data can lead to unbounded memory growth during decompression. This issue has been patched in version 8.0.2. A workaround involves disabling LZMA decompression or limiting response-body-limit size.	7.5	More Details
CVE-	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. In versions from 8.0.0 to before 8.0.2, a NULL		More

2025-64335	dereference can occur when the entropy keyword is used in conjunction with base64_data. This issue has been patched in version 8.0.2. A workaround involves disabling rules that use entropy in conjunction with base64_data.	7.5	Details
CVE-2025-54851	A denial of service vulnerability exists in the Modbus TCP and Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted series of network requests can lead to a denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.An attacker can trigger this denial-of-service condition by sending a single Modbus TCP message to port 503 using the Write Single Register function code (6) to write the value 1 to register 4352. This action changes the Modbus address to 15. After this message is sent, the device will be in a denial-of-service state.	7.5	More Details
CVE-2025-64333	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. Prior to versions 7.0.13 and 8.0.2, a large HTTP content type, when logged can cause a stack overflow crashing Suricata. This issue has been patched in versions 7.0.13 and 8.0.2. A workaround for this issue involves limiting stream.reassembly.depth to less then half the stack size. Increasing the process stack size makes it less likely the bug will trigger.	7.5	More Details
CVE-2025-64332	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. Prior to versions 7.0.13 and 8.0.2, a stack overflow that causes Suricata to crash can occur if SWF decompression is enabled. This issue has been patched in versions 7.0.13 and 8.0.2. A workaround for this issue involves disabling SWF decompression (swf-decompression in suricata.yaml), it is disabled by default; set decompress-depth to lower than half your stack size if swf-decompression must be enabled.	7.5	More Details
CVE-2025-64344	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. Prior to versions 7.0.13 and 8.0.2, working with large buffers in Lua scripts can lead to a stack overflow. Users of Lua rules and output scripts may be affected when working with large buffers. This includes a rule passing a large buffer to a Lua script. This issue has been patched in versions 7.0.13 and 8.0.2. A workaround for this issue involves disabling Lua rules and output scripts, or making sure limits, such as stream.depth.reassembly and HTTP response body limits (response-body-limit), are set to less than half the stack size.	7.5	More Details
CVE-2025-64331	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. Prior to versions 7.0.13 and 8.0.2, a stack overflow can occur on large HTTP file transfers if the user has increased the HTTP response body limit and enabled the logging of printable http bodies. This issue has been patched in versions 7.0.13 and 8.0.2. A workaround for this issue involves using default HTTP response body limits and/or disabling http-body-printable logging; body logging is disabled by default.	7.5	More Details
CVE-2025-54850	A denial of service vulnerability exists in the Modbus TCP and Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted series of network requests can lead to a denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.An attacker can trigger this denial-of-service condition by sending a sequence of Modbus RTU over TCP messages to port 503 using the Write Single Register function code (6). The attack sequence begins with a message to register 58112 with a value of 1000, indicating that a configuration change will follow. Next, a message is sent to register 29440 with a value corresponding to the new Modbus address to be configured. Finally, a message to register 57856 with a value of 161 commits the configuration change. After this configuration change, the device will be in a denial-of-service state.	7.5	More Details
CVE-2025-59789	Uncontrolled recursion in the json2pb component in Apache bRPC (version < 1.15.0) on all platforms allows remote attackers to make the server crash via sending deep recursive json data. Root Cause: The bRPC json2pb component uses rapidjson to parse json data from the network. The rapidjson parser uses a recursive parsing method by default. If the input json has a large depth of recursive structure, the parser function may run into stack overflow. Affected Scenarios: Use bRPC server with protobuf message to serve http+json requests from untrusted network. Or directly use JsonToProtoMessage to convert json from untrusted input. How to Fix: (Choose one of the following options) 1. Upgrade bRPC to version 1.15.0, which fixes this issue. 2. Apply this patch: https://github.com/apache/brpc/pull/3099 Note: No matter which option you choose, you should know that the fix introduces a recursion depth limit with default value 100. It affects these functions: ProtoMessageToJson, ProtoMessageToProtoJson, JsonToProtoMessage, and ProtoJsonToProtoMessage. If your requests contain json or protobuf messages that have a	7.5	More Details

	depth exceeding the limit, the request will be failed after applying the fix. You can modify the gflag json2pb_max_recursion_depth to change the limit.		
CVE-2025-54849	A denial of service vulnerability exists in the Modbus TCP and Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted series of network requests can lead to a denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.An attacker can trigger this denial-of-service condition by sending a single Modbus TCP message to port 502 using the Write Single Register function code (6) to write the value 1 to register 4352. This action changes the Modbus address to 15. After this message is sent, the device will be in a denial-of-service state.	7.5	More Details
CVE-2025-61610	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-51735	CSV formula injection vulnerability in HCL Technologies Ltd. Unica 12.0.0.	7.5	More Details
CVE-2025-11131	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-11132	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-11133	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-3012	In dpc modem, there is a possible system crash due to null pointer dereference. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-61607	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-61608	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-61609	In modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-61617	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-2025-54848	A denial of service vulnerability exists in the Modbus TCP and Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted series of network requests can lead to a denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.An attacker can trigger this denial-of-service condition by sending a sequence of Modbus TCP messages to port 502 using the Write Single Register function code (6). The attack sequence begins with a message to register 58112 with a value of 1000, indicating that a configuration change will follow. Next, a message is sent to register 29440 with a value corresponding to the new Modbus address to be configured. Finally, a message to register 57856 with a value of 161 commits the configuration change. After this configuration change, the device will be in a denial-of-service state.	7.5	More Details
CVE-2025-61618	In nr modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed	7.5	More Details
CVE-	In nr modem, there is a possible system crash due to improper input validation. This could lead		More

2025-61619	to remote denial of service with no additional execution privileges needed	7.5	Details
CVE-2025-41738	An unauthenticated remote attacker may cause the visualisation server of the CODESYS Control runtime system to access a resource with a pointer of wrong type, potentially leading to a denial-of-service (DoS) condition.	7.5	More Details
CVE-2024-56089	An issue in Technitium through v13.2.2 enables attackers to conduct a DNS cache poisoning attack and inject fake responses by reviving the birthday attack.	7.5	More Details
CVE-2025-64330	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. Prior to versions 7.0.13 and 8.0.2, a single byte read heap overflow when logging the verdict in eve.alert and eve.drop records can lead to crashes. This requires the per packet alert queue to be filled with alerts and then followed by a pass rule. This issue has been patched in versions 7.0.13 and 8.0.2. To reduce the likelihood of this issue occurring, the alert queue size a should be increased (packet-alert-max in suricata.yaml) if verdict is enabled.	7.5	More Details
CVE-2025-12758	Versions of the package validator before 13.15.22 are vulnerable to Incomplete Filtering of One or More Instances of Special Elements in the isLength() function that does not take into account Unicode variation selectors (\uFE0F, \uFE0E) appearing in a sequence which lead to improper string length calculation. This can lead to an application using isLength for input validation accepting strings significantly longer than intended, resulting in issues like data truncation in databases, buffer overflows in other system components, or denial-of-service.	7.5	More Details
CVE-2025-66314	Improper Privilege Management vulnerability in ZTE ElasticNet UME R32 on Linux allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects ElasticNet UME R32: ElasticNet_UME_R32_V16.23.20.04.	7.5	More Details
CVE-2024-53684	A cross-site request forgery (csrf) vulnerability exists in the WEBVIEW-M functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted HTTP request can lead to unauthorized access. An attacker can stage a malicious webpage to trigger this vulnerability.	7.5	More Details
CVE-2025-7820	The SKT PayPal for WooCommerce plugin for WordPress is vulnerable to Payment Bypass in all versions up to, and including, 1.4. This is due to the plugin only enforcing client side controls instead of server-side controls when processing payments. This makes it possible for unauthenticated attackers to make confirmed purchases without actually paying for them.	7.5	More Details
CVE-2025-13768	WebITR developed by Uniong has an Authentication Bypass vulnerability, allowing authenticated remote attackers to log into the system as any user by modifying a specific parameter. Attackers must first obtain a user ID to exploit this vulnerability.	7.5	More Details
CVE-2025-64775	Denial of Service vulnerability in Apache Struts, file leak in multipart request processing causes disk exhaustion. This issue affects Apache Struts: from 2.0.0 through 6.7.0, from 7.0.0 through 7.0.3. Users are recommended to upgrade to version 6.8.0 or 7.1.1, which fixes the issue.	7.5	More Details
CVE-2025-65278	An issue was discovered in file users.json in GroceryMart commit 21934e6 (2020-10-23) allowing unauthenticated attackers to gain sensitive information including plaintext usernames and passwords.	7.5	More Details
CVE-2025-13724	The VikRentCar Car Rental Management System plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'month' parameter in all versions up to, and including, 1.4.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-13295	Insertion of Sensitive Information Into Sent Data vulnerability in Argus Technology Inc. BILGER allows Choosing Message Identifier.This issue affects BILGER: before 2.4.9.	7.5	More Details
CVE-2025-64460	An issue was discovered in 5.2 before 5.2.9, 5.1 before 5.1.15, and 4.2 before 4.2.27. Algorithmic complexity in `django.core.serializers.xml_serializer.getInnerText()` allows a remote attacker to cause a potential denial-of-service attack triggering CPU and memory exhaustion via specially crafted XML input processed by the XML `Deserializer`. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to	7.5	More Details

	thank Seokchan Yoon for reporting this issue.		
CVE-2025-55471	Incorrect access control in the getUserFormData function of youlai-boot v2.21.1 allows attackers to access sensitive information for other users.	7.5	More Details
CVE-2025-65672	Insecure Direct Object Reference (IDOR) in classroomio 0.1.13 allows unauthorized share and invite access to course settings.	7.5	More Details
CVE-2025-66020	Valibot helps validate data using a schema. In versions from 0.31.0 to 1.1.0, the EMOJI_REGEX used in the emoji action is vulnerable to a Regular Expression Denial of Service (ReDoS) attack. A short, maliciously crafted string (e.g., <100 characters) can cause the regex engine to consume excessive CPU time (minutes), leading to a Denial of Service (DoS) for the application. This issue has been patched in version 1.2.0.	7.5	More Details
CVE-2025-13721	Race in v8 in Google Chrome prior to 143.0.7499.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2025-61729	Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.	7.5	More Details
CVE-2025-12571	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.10 before 18.4.5, 18.5 before 18.5.3, and 18.6 before 18.6.1 that could have allowed an unauthenticated user to cause a Denial of Service condition by sending specifically crafted requests containing malicious JSON payloads.	7.5	More Details
CVE-2025-7007	NULL Pointer Dereference vulnerability in Avast Antivirus on MacOS, Avast Anitvirus on Linux when scanning a malformed Windows PE file causes the antivirus process to crash.This issue affects Antivirus: 16.0.0; Anitvirus: 3.0.3.	7.5	More Details
CVE-2025-13735	Out-of-bounds Read vulnerability in ASR1903、ASR3901 in ASR Lapwing_Linux on Linux (nr_fw modules). This vulnerability is associated with program files Code/nr_fw/DLP/src/NrCgi.C. This issue affects Lapwing_Linux: before 2025/11/26.	7.4	More Details
CVE-2025-13808	A flaw has been found in orionsec orion-ops up to 5925824997a3109651bbde07460958a7be249ed1. Affected by this vulnerability is the function update of the file orion-ops-api/orion-ops-web/src/main/java/cn/orionsec/ops/controller/UserController.java of the component User Profile Handler. This manipulation of the argument ID causes improper authorization. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-45370	An authentication bypass vulnerability exists in the User profile management functionality of Socomec Easy Config System 2.6.1.0. A specially crafted database record can lead to unauthorized access. An attacker can modify a local database to trigger this vulnerability.	7.3	More Details
CVE-2025-13806	A security vulnerability has been detected in nutzam NutzBoot up to 2.6.0-SNAPSHOT. This impacts an unknown function of the file nutzboot-demo/nutzboot-demo-simple/nutzboot-demo-simple-web3j/src/main/java/io/nutz/demo/simple/module/EthModule.java of the component Transaction API. The manipulation of the argument from/to/wei leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13803	A vulnerability was identified in MediaCrush 1.0.0/1.0.1. The affected element is an unknown function of the file /mediacrush/paths.py of the component Header Handler. Such manipulation of the argument Host leads to improper neutralization of http headers for scripting syntax. The attack can be launched remotely.	7.3	More Details
CVE-2025-13792	A security flaw has been discovered in Qualitor up to 8.20.104/8.24.97. Affected by this vulnerability is the function eval of the file /html/st/stdeslocamento/request/getResumo.php. Performing manipulation of the argument passageiros results in code injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. Upgrading to version 8.20.105 and 8.24.98 addresses this issue. Upgrading the	7.3	More Details

	affected component is advised.		
CVE-2025-13814	A security flaw has been discovered in moxi159753 Mogu Blog v2 up to 5.2. Impacted is the function LocalFileServiceImpl.uploadPictureByUrl of the file /file/uploadPicsByUrl. The manipulation results in server-side request forgery. The attack can be launched remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-13788	A vulnerability has been found in Chanjet CRM up to 20251106. The impacted element is an unknown function of the file /tools/upgradeattribute.php. The manipulation of the argument gblOrgID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-59890	Improper input sanitization in the file archives upload functionality of Eaton Galileo software allows traversing paths which could lead into an attacker with local access to execute unauthorized code or commands. This security issue has been fixed in the latest version of Galileo which is available on the Eaton download center.	7.3	More Details
CVE-2025-13786	A vulnerability was detected in taosir WTCMS up to 01a5f68a3dfc2fdddb44eed967bb2d4f60487665. Impacted is the function fetch of the file /index.php. Performing manipulation of the argument content results in code injection. It is possible to initiate the attack remotely. The exploit is now 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. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-13782	A vulnerability was identified in taosir WTCMS up to 01a5f68a3dfc2fdddb44eed967bb2d4f60487665. Affected by this issue is the function delete of the file application/Admin/Controller/SlideController.class.php of the component SlideController. The manipulation of the argument ids leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-58316	DoS vulnerability in the video-related system service module. Impact: Successful exploitation of this vulnerability may affect availability.	7.3	More Details
CVE-2025-64778	NMIS/BioDose software V22.02 and previous versions contain executable binaries with plain text hard-coded passwords. These hard-coded passwords could allow unauthorized access to both the application and database.	7.3	More Details
CVE-2025-58308	Vulnerability of improper criterion security check in the call module. Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	7.3	More Details
CVE-2025-58481	Improper access control in MPRemoteService of MotionPhoto prior to version 4.1.51 allows local attackers to start privileged service.	7.3	More Details
CVE-2025-58482	Improper access control in MPLocalService of MotionPhoto prior to version 4.1.51 allows local attackers to start privileged service.	7.3	More Details
CVE-2024-49572	A denial of service vulnerability exists in the Modbus TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to denial of service and weaken credentials resulting in default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability.	7.2	More Details
CVE-2025-13387	The Kadence WooCommerce Email Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the customer name in all versions up to, and including, 1.5.17 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-2025-13692	The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads 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 will execute whenever a user accesses the SVG file. A form with a file upload field must be created with the premium version of the plugin in order to exploit the vulnerability. However, once the form exists, the vulnerability is exploitable even if the premium version is deactivated and/or uninstalled.	7.2	More Details
CVE-2025-59702	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a physically proximate attacker with elevated privileges to falsify tamper events by accessing internal components.	7.2	More Details
CVE-2025-20085	A denial of service vulnerability exists in the Modbus RTU over TCP functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted network packet can lead to denial of service and weaken credentials resulting in default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability.	7.2	More Details
CVE-2025-53899	Kiteworks MFT orchestrates end-to-end file transfer workflows. Prior to version 9.1.0, the back-end of Kiteworks MFT is vulnerable to an incorrectly specified destination in a communication channel which allows an attacker with administrative privileges on the system under certain circumstances to intercept upstream communication which could lead to an escalation of privileges. This issue has been patched in version 9.1.0.	7.2	More Details
CVE-2025-59697	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a physically proximate attacker to escalate privileges by editing the Legacy GRUB bootloader configuration to start a root shell upon boot of the host OS. This is called F06.	7.2	More Details
CVE-2025-11699	nopCommerce v4.70 and prior, and version 4.80.3, does not invalidate session cookies after logout or session termination, allowing an attacker who has a a valid session cookie access to privileged endpoints (such as /admin) even after the legitimate user has logged out, enabling session hijacking. Any version above 4.70 that is not 4.80.3 fixes the vulnerability.	7.1	More Details
CVE-2025-66423	Tryton trytond 6.0 before 7.6.11 does not enforce access rights for the route of the HTML editor. This is fixed in 7.6.11, 7.4.21, 7.0.40, and 6.0.70.	7.1	More Details
CVE-2025-63365	SoftSea EPUB File Reader 1.0.0.0 is vulnerable to Directory Traversal. The vulnerability resides in the EPUB file processing component, specifically in the functionality responsible for extracting and handling EPUB archive contents.	7.1	More Details
CVE-2025-66205	Frappe is a full-stack web application framework. Prior to 15.86.0 and 14.99.2, a certain endpoint was vulnerable to error-based SQL injection due to lack of validation of parameters. Some information like version could be retrieved. This vulnerability is fixed in 15.86.0 and 14.99.2.	7.1	More Details
CVE-2025-66448	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.11.1, vllm has a critical remote code execution vector in a config class named Nemotron_Nano_VL_Config. When vllm loads a model config that contains an auto_map entry, the config class resolves that mapping with get_class_from_dynamic_module(...) and immediately instantiates the returned class. This fetches and executes Python from the remote repository referenced in the auto_map string. Crucially, this happens even when the caller explicitly sets trust_remote_code=False in vllm.transformers_utils.config.get_config. In practice, an attacker can publish a benign-looking frontend repo whose config.json points via auto_map to a separate malicious backend repo; loading the frontend will silently run the backend’s code on the victim host. This vulnerability is fixed in 0.11.1.	7.1	More Details
CVE-2025-53896	Kiteworks MFT orchestrates end-to-end file transfer workflows. Prior to version 9.1.0, a bug in Kiteworks MFT could cause under certain circumstances that a user's active session would not properly time out due to inactivity. This issue has been patched in version 9.1.0.	7.1	More Details
CVE-2025-66302	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, A path traversal vulnerability has been identified in Grav CMS, allowing authenticated attackers with administrative privileges to read arbitrary files on the underlying server filesystem. This vulnerability arises due to insufficient input sanitization in the backup tool, where user-supplied paths are not properly restricted, enabling access to files outside the intended webroot directory. The impact of this vulnerability depends on the privileges of the user account running the application. This vulnerability is fixed in 1.8.0-beta.27.	6.8	More Details

CVE-2025-66206	Frappe is a full-stack web application framework. Prior to 15.86.0 and 14.99.2, certain requests were vulnerable to path traversal attacks, wherein some files from the server could be retrieved if the full path was known. Sites hosted on Frappe Cloud, and even other setups that are behind a reverse proxy like NGINX are unaffected. This would mainly affect someone directly using werkzeug/gunicorn. In those cases, either an upgrade or changing the setup to use a reverse proxy is recommended. This vulnerability is fixed in 15.86.0 and 14.99.2.	6.8	More Details
CVE-2024-32384	Kerlink gateways running KerOS prior to version 5.10 expose their web interface exclusively over HTTP, without HTTPS support. This lack of transport layer security allows a man-in-the-middle attacker to intercept and modify traffic between the client and the device.	6.8	More Details
CVE-2025-53897	Kiteworks MFT orchestrates end-to-end file transfer workflows. Prior to version 9.1.0, this vulnerability could allow an external attacker to gain access to log information from the system by tricking an administrator into browsing a specifically crafted fake page of Kiteworks MFT. This issue has been patched in version 9.1.0.	6.8	More Details
CVE-2025-58309	Permission control vulnerability in the startup recovery module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	6.8	More Details
CVE-2025-20774	In display, 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: ALPS10196993; Issue ID: MSV-4796.	6.7	More Details
CVE-2025-20772	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10196993; Issue ID: MSV-4801.	6.7	More Details
CVE-2025-20775	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182914; Issue ID: MSV-4795.	6.7	More Details
CVE-2025-59820	In KDE Krita before 5.2.13, loading a manipulated TGA file could result in a heap-based buffer overflow in plugins/impex/tga/kis_tga_import.cpp (aka KisTgaImport). Control flow proceeds even when a number of pixels becomes negative.	6.7	More Details
CVE-2025-20771	In display, there is a possible escalation of privilege due to improper input validation. 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: ALPS10196993; Issue ID: MSV-4802.	6.7	More Details
CVE-2025-20777	In display, 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: ALPS10184870; Issue ID: MSV-4752.	6.7	More Details
CVE-2025-20773	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10196993; Issue ID: MSV-4797.	6.7	More Details
CVE-2025-20776	In display, there is a possible out of bounds read 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: ALPS10184297; Issue ID: MSV-4759.	6.7	More Details
CVE-2025-20770	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10196993; Issue ID: MSV-4803.	6.7	More Details
CVE-2025-58314	Vulnerability of accessing invalid memory in the component driver module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	6.6	More Details
CVE-2025-11772	A carefully crafted DLL, copied to C:\ProgramData\Synaptics folder, allows a local user to execute arbitrary code with elevated privileges during driver installation.	6.6	More Details
CVE-2025-	WebITR developed by Uniong has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details

13769			
CVE-2025-13770	WebITR developed by Uniong has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2025-13771	WebITR developed by Uniong has an Arbitrary File Read vulnerability, allowing authenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	6.5	More Details
CVE-2025-65113	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.2 - #164, an authorization bypass vulnerability in the AJAX flagging system allows any unauthenticated user to flag any content (users, videos, photos, collections) on the platform. This can lead to mass flagging attacks, content disruption, and moderation system abuse. This issue has been patched in version 5.5.2 - #164.	6.5	More Details
CVE-2025-65657	FeehiCMS version 2.1.1 has a Remote Code Execution via Unrestricted File Upload in Ad Management. FeehiCMS version 2.1.1 allows authenticated remote attackers to upload files that the server later executes (or stores in an executable location) without sufficient validation, sanitization, or execution restrictions. An authenticated remote attacker can upload a crafted PHP file and cause the application or web server to execute it, resulting in remote code execution (RCE).	6.5	More Details
CVE-2025-65380	PHPGurukul Billing System 1.0 is vulnerable to SQL Injection in the admin/index.php endpoint. Specifically, the username parameter accepts unvalidated user input, which is then concatenated directly into a backend SQL query.	6.5	More Details
CVE-2025-53900	Kiteworks MFT orchestrates end-to-end file transfer workflows. Prior to version 9.1.0, an unfavourable definition of roles and permissions in Kiteworks MFT on managing Connections could lead to unexpected escalation of privileges for authorized users. This issue has been patched in version 9.1.0.	6.5	More Details
CVE-2025-13683	Exposure of credentials in unintended requests in Devolutions Server, Remote Desktop Manager on Windows.This issue affects Devolutions Server: through 2025.3.8.0; Remote Desktop Manager: through 2025.3.23.0.	6.5	More Details
CVE-2025-12483	The Visualizer: Tables and Charts Manager for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'query' parameter in all versions up to, and including, 3.11.12 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Version 3.11.13 raises the minimum user-level for exploitation to administrator. 3.11.14 fully patches the vulnerability.	6.5	More Details
CVE-2025-66424	Tryton trytond 6.0 before 7.6.11 does not enforce access rights for data export. This is fixed in 7.6.11, 7.4.21, 7.0.40, and 6.0.70.	6.5	More Details
CVE-2025-65877	Lvzhou CMS before commit c4ea0eb9cab5f6739b2c87e77d9ef304017ed615 (2025-09-22) is vulnerable to SQL injection via the 'title' parameter in com.wanli.lvzhoucms.service.ContentService#findPage. The parameter is concatenated directly into a dynamic SQL query without sanitization or prepared statements, enabling attackers to read sensitive data from the database.	6.5	More Details
CVE-2025-65405	A use-after-free in the ADTSAudioFileSource::samplingFrequency() function of Live555 Streaming Media v2018.09.02 allows attackers to cause a Denial of Service (DoS) via supplying a crafted ADTS/AAC file.	6.5	More Details
CVE-2025-65406	A heap overflow in the MatroskaFile::createRTPSinkForTrackNumber() function of Live555 Streaming Media v2018.09.02 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MKV file.	6.5	More Details
CVE-2025-65408	A NULL pointer dereference in the ADTSAudioFileServerMediaSubsession::createNewRTPSink() function of Live555 Streaming Media v2018.09.02 allows attackers to cause a Denial of Service (DoS) via supplying a crafted ADTS file.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability		

2025-13835	in Tyche Softwares Arconix Shortcodes allows Stored XSS.This issue affects Arconix Shortcodes: from n/a through 2.1.19.	6.5	More Details
CVE-2025-63095	Improper input validation in the BitstreamWriter::write_bits() function of Tempus Ex hello-video-codec v0.1.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details
CVE-2025-65407	A use-after-free in the MPEG1or2Demux::newElementaryStream() function of Live555 Streaming Media v2018.09.02 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MPEG Program stream.	6.5	More Details
CVE-2025-66307	This admin plugin for Grav is an HTML user interface that provides a convenient way to configure Grav and easily create and modify pages. Prior to 1.11.0-beta.1, a user enumeration and email disclosure vulnerability exists in Grav. The "Forgot Password" functionality at /admin/forgot leaks information about valid usernames and their associated email addresses through distinct server responses. This allows an attacker to enumerate users and disclose sensitive email addresses, which can be leveraged for targeted attacks such as password spraying, phishing, or social engineering. This vulnerability is fixed in 1.11.0-beta.1.	6.5	More Details
CVE-2025-20752	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01270690; Issue ID: MSV-4301.	6.5	More Details
CVE-2025-20759	In Modem, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01673760; Issue ID: MSV-4650.	6.5	More Details
CVE-2025-63523	FeehiCMS version 2.1.1 fails to enforce server-side immutability for parameters that are presented to clients as "read-only." An authenticated attacker can intercept and modify the parameter in transit and the backend accepts the changes. This can lead to unintended username changes.	6.5	More Details
CVE-2025-13606	The Export All Posts, Products, Orders, Refunds & Users plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.19. This is due to missing or incorrect nonce validation on the `parseData` function. This makes it possible for unauthenticated attackers to export sensitive information including user data, email addresses, password hashes, and WooCommerce data to an attacker-controlled file path on the server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2025-65404	A buffer overflow in the getSideInfo2() function of Live555 Streaming Media v2018.09.02 allows attackers to cause a Denial of Service (DoS) via a crafted MP3 stream.	6.5	More Details
CVE-2025-58113	An out-of-bounds read vulnerability exists in the EMF functionality of PDF-XChange Co. Ltd PDF-XChange Editor 10.7.3.401. 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-2025-66454	Arcade MCP allows you to to create, deploy, and share MCP Servers. Prior to 1.5.4, the arcade-mcp HTTP server uses a hardcoded default worker secret ("dev") that is never validated or overridden during normal server startup. As a result, any unauthenticated attacker who knows this default key can forge valid JWTs and fully bypass the FastAPI authentication layer. This grants remote access to all worker endpoints—including tool enumeration and tool invocation—without credentials. This vulnerability is fixed in 1.5.4.	6.5	More Details
CVE-2025-65379	PHPGurukul Billing System 1.0 is vulnerable to SQL Injection in the /admin/password-recovery.php endpoint. Specifically, the username and mobileno parameters accepts unvalidated user input, which is then concatenated directly into a backend SQL query.	6.5	More Details
CVE-2025-65403	A buffer overflow in the g_cfg.MaxUsers component of LightFTP v2.0 allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details

CVE-2025-65956	Formwork is a flat file-based Content Management System (CMS). Prior to version 2.2.0, inserting unsanitized data into the blog tag field results in stored cross-site scripting (XSS). Any user with credentials to the Formwork CMS who accesses or edits an affected blog post will have attacker-controlled script executed in their browser. The issue is persistent and impacts privileged administrative workflows. This issue has been patched in version 2.2.0.	6.5	More Details
CVE-2021-4472	The mistral-dashboard plugin for openstack has a local file inclusion vulnerability through the 'Create Workbook' feature that may result in disclosure of arbitrary local files content.	6.5	More Details
CVE-2025-7449	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.3 before 18.4.5, 18.5 before 18.5.3, and 18.6 before 18.6.1 that could have allowed an authenticated user with specific permissions to cause a denial of service condition through HTTP response processing.	6.5	More Details
CVE-2025-13378	The AI ChatBot with ChatGPT and Content Generator by AYS plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.7.0 via the ays_chatgpt_pinecone_upsert function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	6.5	More Details
CVE-2025-63938	Tinyproxy through 1.11.2 contains an integer overflow vulnerability in the strip_return_port() function within src/reqs.c.	6.5	More Details
CVE-2025-12653	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.3 before 18.4.5, 18.5 before 18.5.3, and 18.6 before 18.6.1 that under specific conditions could have allowed an unauthenticated user to join arbitrary organizations by changing headers on some requests.	6.5	More Details
CVE-2025-12649	The SortTable Post plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in the sorttablepost shortcode in all versions up to, and including, 4.2. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page via mouse interaction.	6.4	More Details
CVE-2025-13697	The BlockArt Blocks – Gutenberg Blocks, Page Builder Blocks ,WordPress Block Plugin, Sections & Template Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘timestamp’ attribute in all versions up to, and including, 2.2.13 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-2025-12670	The wp-twitpic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters of the 'twitpic' shortcode 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-2025-12712	The Shouty plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the shouty shortcode in all versions up to, and including, 0.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12713	The Soundslides plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the soundslides shortcode in all versions up to, and including, 1.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12151	The Simple Folio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'portfolio_name' parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-			

2025-58307	UAF vulnerability in the screen recording framework module. Impact: Successful exploitation of this vulnerability may affect availability.	6.4	More Details
CVE-2025-13731	The Nexter Extension – Site Enhancements Toolkit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'nxt-year' shortcode in all versions up to, and including, 4.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12666	The Google Drive upload and download link plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter of the 'atachfilegoogle' shortcode 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-2025-53939	Kiteworks is a private data network (PDN). Prior to version 9.1.0, improper input validation when managing roles of a shared folder could lead to unexpectedly elevate another user's permissions on the share. This issue has been patched in version 9.1.0.	6.3	More Details
CVE-2025-13809	A vulnerability has been found in orionsec orion-ops up to 5925824997a3109651bbde07460958a7be249ed1. Affected by this issue is some unknown functionality of the file orion-ops-api/orion-ops-web/src/main/java/cn/orionsec/ops/controller/MachineInfoController.java of the component SSH Connection Handler. Such manipulation of the argument host/sshPort/username/password/authType leads to server-side request forgery. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. A patch should be applied to remediate this issue. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13534	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.3.2. This is due to missing authorization checks on the eh_crm_edit_agent AJAX action. This makes it possible for authenticated attackers, with Contributor-level access and above, to escalate their WSDesk privileges from limited "Reply Tickets" permissions to full helpdesk administrator capabilities, gaining unauthorized access to ticket management, settings configuration, agent administration, and sensitive customer data.	6.3	More Details
CVE-2025-13789	A vulnerability was found in ZenTao up to 21.7.6-8564. This affects the function makeRequest of the file module/ai/model.php. The manipulation of the argument Base results in server-side request forgery. The attack can be launched remotely. The exploit has been made public and could be used. Upgrading to version 21.7.6 mitigates this issue. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2025-13791	A vulnerability was identified in Scada-LTS up to 2.7.8.1. Affected is the function Common.getHomeDir of the file br/org/scadabr/vo/exporter/ZIPProjectManager.java of the component Project Import. Such manipulation leads to path traversal. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13816	A security vulnerability has been detected in moxi159753 Mogu Blog v2 up to 5.2. The impacted element is the function FileOperation.unzip of the file /networkDisk/unzipFile of the component ZIP File Handler. Such manipulation of the argument fileUrl leads to path traversal. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13796	A security vulnerability has been detected in deco-cx apps up to 0.120.1. Affected by this vulnerability is the function AnalyticsScript of the file website/loaders/analyticsScript.ts of the component Parameter Handler. Such manipulation of the argument url leads to server-side request forgery. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.120.2 addresses this issue. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2025-13797	A vulnerability was detected in ADSLR B-QE2W401 250814-r037c. Affected by this issue is the function parameterdel_swifimac of the file /send_order.cgi. Performing manipulation of the argument del_swifimac results in command injection. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this	6.3	More Details

	disclosure but did not respond in any way.		
CVE-2025-13798	A flaw has been found in ADSLR NBR1005GPEV2 250814-r037c. This affects the function ap_macfilter_add of the file /send_order.cgi. Executing manipulation of the argument mac can lead to command injection. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13799	A vulnerability has been found in ADSLR NBR1005GPEV2 250814-r037c. This vulnerability affects the function ap_macfilter_del of the file /send_order.cgi. The manipulation of the argument mac leads to command 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-2025-13815	A weakness has been identified in moxi159753 Mogu Blog v2 up to 5.2. The affected element is an unknown function of the file /file/pictures. This manipulation of the argument filedatas causes unrestricted upload. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13800	A vulnerability was found in ADSLR NBR1005GPEV2 250814-r037c. This issue affects the function set_mesh_disconnect of the file /send_order.cgi. The manipulation of the argument mac results in command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13875	A weakness has been identified in Yohann0617 oci-helper up to 3.2.4. This issue affects the function addCfg of the file src/main/java/com/yohann/ocihelper/service/impl/OciServiceImpl.java of the component OCI Configuration Upload. Executing manipulation of the argument File can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13783	A security flaw has been discovered in taosir WTCMS up to 01a5f68a3dfc2fdddb44eed967bb2d4f60487665. This affects the function check/uncheck/delete of the file application/Comment/Controller/CommentadminController.class.php of the component CommentadminController. The manipulation of the argument ids results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13811	A vulnerability was determined in jsnjfz WebStack-Guns 1.0. This vulnerability affects unknown code of the file src/main/java/com/jsnjfz/manage/core/common/constant/factory/PageFactory.java. Executing manipulation of the argument sort can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-51736	File upload vulnerability in HCL Technologies Ltd. Unica 12.0.0.	6.3	More Details
CVE-2025-66034	fontTools is a library for manipulating fonts, written in Python. In versions from 4.33.0 to before 4.60.2, the fonttools varLib (or python3 -m fontTools.varLib) script has an arbitrary file write vulnerability that leads to remote code execution when a malicious .designspace file is processed. The vulnerability affects the main() code path of fontTools.varLib, used by the fonttools varLib CLI and any code that invokes fontTools.varLib.main(). This issue has been patched in version 4.60.2.	6.3	More Details
CVE-2025-9191	The Houzez theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.1.6 via deserialization of untrusted input in saved-search-item.php. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a	6.3	More Details

	POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.		
CVE-2025-21080	Improper export of android application components in Dynamic Lockscreen prior to SMR Dec-2025 Release 1 allows local attackers to access files with Dynamic Lockscreen's privilege.	6.2	More Details
CVE-2025-58305	Identity authentication bypass vulnerability in the Gallery app. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2025-58294	Permission control vulnerability in the print module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2025-66304	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, users with read access on the user account management section of the admin panel can view the password hashes of all users, including the admin user. This exposure can potentially lead to privilege escalation if an attacker can crack these password hashes. This vulnerability is fixed in 1.8.0-beta.27.	6.2	More Details
CVE-2025-65187	A Stored Cross Site Scripting vulnerability exists in CiviCRM before v6.7 in the Accounting Batches field. An authenticated user can inject malicious JavaScript into this field and it executes whenever the page is viewed.	6.1	More Details
CVE-2025-12143	Stack-based Buffer Overflow vulnerability in ABB Terra AC wallbox.This issue affects Terra AC wallbox: through 1.8.33.	6.1	More Details
CVE-2025-66026	REDAXO is a PHP-based CMS. Prior to version 5.20.1, a reflected Cross-Site Scripting (XSS) vulnerability exists in the Mediapool view where the request parameter args[types] is rendered into an info banner without HTML-escaping. This allows arbitrary JavaScript execution in the backend context when an authenticated user visits a crafted link while logged in. This issue has been patched in version 5.20.1.	6.1	More Details
CVE-2025-63872	DeepSeek V3.2 has a Cross Site Scripting (XSS) vulnerability, which allows JavaScript execution through model-generated SVG content.	6.1	More Details
CVE-2025-13007	The WP Social Ninja – Embed Social Feeds, Customer Reviews, Chat Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.20.3 due to insufficient input sanitization and output escaping on externally-sourced content. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, granted they can post malicious content to a connected Google Business Profile or Facebook page.	6.1	More Details
CVE-2025-63520	Cross Site Scripting (XSS) vulnerability in FeehiCMS 2.1.1 via the id parameter of the User Update function (?r=user%2Fupdate).	6.1	More Details
CVE-2025-13525	The WP Directory Kit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'order_by' parameter in all versions up to, and including, 1.4.5 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-2025-63529	A session fixation vulnerability exists in Blood Bank Management System 1.0 in login.php that allows an attacker to set or predict a user's session identifier prior to authentication. When the victim logs in, the application continues to use the attacker-supplied session ID rather than generating a new one, enabling the attacker to hijack the authenticated session and gain unauthorized access to the victim's account.	6.1	More Details
CVE-2025-12123	The Customer Reviews Collector for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'email-text' parameter in all versions up to, and including, 4.6.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE-2025-59025	Malicious e-mail content can be used to execute script code. Unintended actions can be executed in the context of the users account, including exfiltration of sensitive information. Sanitization has been updated to avoid such bypasses. No publicly available exploits are known	6.1	More Details
CVE-2025-65186	Grav CMS 1.7.49 is vulnerable to Cross Site Scripting (XSS). The page editor allows authenticated users to edit page content via a Markdown editor. The editor fails to properly sanitize <script> tags, allowing stored XSS payloads to execute when pages are viewed in the admin interface.	6.1	More Details
CVE-2025-9163	The Houzez theme for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 4.1.6 due to insufficient input sanitization and output escaping in the houzez_property_img_upload() and houzez_property_attachment_upload() functions. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.1	More Details
CVE-2025-65892	Reflected Cross-Site Scripting (rXSS) in krpano before version 1.23.2 allows a remote unauthenticated attacker to execute arbitrary JavaScript in the victim's browser via a crafted URL to the passQueryParameters function with the xml parameter enabled.	6.1	More Details
CVE-2025-65540	Multiple Cross-Site Scripting (XSS) vulnerabilities exist in xmall v1.1 due to improper handling of user-supplied data. User input fields such as username and description are directly rendered into HTML without proper sanitization or encoding, allowing attackers to inject and execute malicious scripts.	6.1	More Details
CVE-2025-65215	Sourcecodester Web-based Pharmacy Product Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in /product_expiry/add-supplier.php via the Supplier Name field.	6.1	More Details
CVE-2025-65881	Sourcecodester Zoo Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in /classes/Login.php.	6.1	More Details
CVE-2025-66036	Retro is an online platform providing items of vintage collections. Prior to version 2.4.7, Retro is vulnerable to a cross-site scripting (XSS) in the input handling component. This issue has been patched in version 2.4.7.	6.1	More Details
CVE-2025-54057	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Apache SkyWalking. This issue affects Apache SkyWalking: <= 10.2.0. Users are recommended to upgrade to version 10.3.0, which fixes the issue.	6.1	More Details
CVE-2025-13819	Open redirect in the web server component of MiR Robot and Fleet software allows a remote attacker to redirect users to arbitrary external websites via a crafted parameter, facilitating phishing or social engineering attacks.	6.1	More Details
CVE-2025-61915	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. Prior to version 2.4.15, a user in the lpadmin group can use the cups web ui to change the config and insert a malicious line. Then the cupsd process which runs as root will parse the new config and cause an out-of-bound write. This issue has been patched in version 2.4.15.	6.0	More Details
CVE-2025-41739	An unauthenticated remote attacker, who beats a race condition, can exploit a flaw in the communication servers of the CODESYS Control runtime system on Linux and QNX to trigger an out-of-bounds read via crafted socket communication, potentially causing a denial of service.	5.9	More Details
CVE-2024-48894	A cleartext transmission vulnerability exists in the WEBVIEW-M functionality of Socomec DIRIS Digiware M-70 1.6.9. A specially crafted HTTP request can lead to a disclosure of sensitive information. An attacker can sniff network traffic to trigger this vulnerability.	5.9	More Details
CVE-2025-58408	Software installed and run as a non-privileged user may conduct improper GPU system calls to trigger reads of stale data that can lead to kernel exceptions and write use-after-free. The Use After Free common weakness enumeration was chosen as the stale data can include handles to resources in which the reference counts can become unbalanced. This can lead to the premature destruction of a resource while in use.	5.9	More Details
CVE-2025-58483	Improper export of android application components in Galaxy Store for Galaxy Watch prior to version 1.0.06.29 allows local attacker to install arbitrary application on Galaxy Store.	5.9	More Details

CVE-2025-58311	UAF vulnerability in the USB driver module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	5.8	More Details
CVE-2025-21072	Out-of-bounds write in decoding metadata in fingerprint trustlet prior to SMR Dec-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.	5.7	More Details
CVE-2025-13877	A vulnerability was detected in nocobase up to 1.9.4/2.0.0-alpha.37. The affected element is an unknown function of the file nocobase\packages\core\auth\src\base\jwt-service.ts of the component JWT Service. The manipulation of the argument API_KEY results in use of hard-coded cryptographic key . The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is described as difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2025-58475	Improper input validation in libsec-ril.so prior to SMR Dec-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.	5.6	More Details
CVE-2025-13813	A vulnerability was identified in moxi159753 Mogu Blog v2 up to 5.2. This issue affects some unknown processing of the file /storage/ of the component Storage Management Endpoint. The manipulation leads to missing authorization. The attack can be initiated remotely. The attack's complexity is rated as high. The exploitability is assessed as difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2025-51733	Cross-Site Request Forgery (CSRF) vulnerability in HCL Technologies Ltd. Unica 12.0.0.	5.5	More Details
CVE-2025-58485	Improper input validation in Samsung Internet prior to version 29.0.0.48 allows local attackers to inject arbitrary script.	5.5	More Details
CVE-2025-3784	Cleartext Storage of Sensitive Information Vulnerability in GX Works2 all versions allows an attacker to disclose credential information stored in plaintext from project files. As a result, the attacker may be able to open project files protected by user authentication using disclosed credential information, and obtain or modify project information.	5.5	More Details
CVE-2025-13674	BPv7 dissector crash in Wireshark 4.6.0 allows denial of service	5.5	More Details
CVE-2025-58315	Permission control vulnerability in the Wi-Fi module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2025-65676	Stored Cross site scripting (XSS) vulnerability in Classroomio LMS 0.1.13 allows authenticated attackers to execute arbitrary code via crafted SVG cover images.	5.4	More Details
CVE-2025-13296	Cross-Site Request Forgery (CSRF) vulnerability in Tekrom Technology Inc. T-Soft E-Commerce allows Cross Site Request Forgery.This issue affects T-Soft E-Commerce: through 28112025.	5.4	More Details
CVE-2025-63317	Todoist v8896 is vulnerable to Cross Site Scripting (XSS) in /api/v1/uploads. Uploaded SVG files have no sanitization applied, so embedded JavaScript executes when a user opens the attachment from a task/comment.	5.4	More Details
CVE-2025-65675	Stored Cross site scripting (XSS) vulnerability in Classroomio LMS 0.1.13 allows authenticated attackers to execute arbitrary code via crafted SVG profile pictures.	5.4	More Details
CVE-2025-64030	Eximbills Enterprise 4.1.5 (Built on 2020-10-30) is vulnerable to authenticated stored cross-site scripting (CWE-79) via the /EximBillWeb/servlets/WSTrxManager endpoint. Unsanitized user input in the TMPL_INFO parameter is stored server-side and rendered to other users, enabling arbitrary	5.4	More Details

	JavaScript execution in their browsers.		
CVE-2025-30190	Malicious content at office documents can be used to inject script code when editing a document. Unintended actions can be executed in the context of the users account, including exfiltration of sensitive information. Please deploy the provided updates and patch releases. No publicly available exploits are known	5.4	More Details
CVE-2025-59026	Malicious content uploaded as file can be used to execute script code when following attacker-controlled links. Unintended actions can be executed in the context of the users account, including exfiltration of sensitive information. Please deploy the provided updates and patch releases. No publicly available exploits are known	5.4	More Details
CVE-2025-62728	SQL injection vulnerability in Hive Metastore Server (HMS) when processing delete column statistics requests via the Thrift APIs. The vulnerability is only exploitable by trusted/authorized users/applications that are allowed to call directly the Thrift APIs. In most real-world deployments, HMS is accessible to only a handful of applications (e.g., Hiveserver2) thus the vulnerability is not exploitable. Moreover, the vulnerable code cannot be reached when metastore.try.direct.sql property is set to false. This issue affects Apache Hive: from 4.1.0 before 4.2.0. Users are recommended to upgrade to version 4.2.0, which fixes the issue. Users who cannot upgrade directly are encouraged to set metastore.try.direct.sql property to false if the HMS Thrift APIs are exposed to general public.	5.4	More Details
CVE-2025-30186	Malicious content uploaded as file can be used to execute script code when following attacker-controlled links. Unintended actions can be executed in the context of the users account, including exfiltration of sensitive information. Please deploy the provided updates and patch releases. No publicly available exploits are known	5.4	More Details
CVE-2025-64070	Sourcecodester Student Grades Management System v1.0 is vulnerable to Cross Site Scripting (XSS) in the Add New Subject Description field.	5.4	More Details
CVE-2025-66421	Tryton sao (aka tryton-sao) before 7.6.11 allows XSS because it does not escape completion values. This is fixed in 7.6.11, 7.4.21, 7.0.40, and 6.0.69.	5.4	More Details
CVE-2025-13787	A flaw has been found in ZenTao up to 21.7.6-8564. The affected element is the function file::delete of the file module/file/control.php of the component File Handler. Executing manipulation of the argument fileID can lead to improper privilege management. It is possible to launch the attack remotely. Upgrading to version 21.7.7 is sufficient to fix this issue. You should upgrade the affected component.	5.4	More Details
CVE-2025-59790	Improper Privilege Management vulnerability in Apache Kvrocks. This issue affects Apache Kvrocks: from v2.9.0 through v2.13.0. Users are recommended to upgrade to version 2.14.0, which fixes the issue.	5.4	More Details
CVE-2025-13632	Inappropriate implementation in DevTools in Google Chrome prior to 143.0.7499.41 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: High)	5.4	More Details
CVE-2025-51734	Cross-site scripting (XSS) vulnerability in HCL Technologies Ltd. Unica 12.0.0.	5.4	More Details
CVE-2025-52622	The BigFix SaaS's HTTP responses were missing some security headers. The absence of these headers weakens the application's client-side security posture, making it more vulnerable to common web attacks that these headers are designed to mitigate, such as Cross-Site Scripting (XSS), Clickjacking, and protocol downgrade attacks.	5.4	More Details
CVE-2025-65963	Files is a module for managing files inside spaces and user profiles. Prior to versions 0.16.11 and 0.17.2, insufficient authorization checks allow non-member users to create new folders, up- and download files as a ZIP archive in public spaces. Private spaces are not affected. This issue has been patched in versions 0.16.11 and 0.17.2.	5.4	More Details
CVE-2025-66420	Tryton sao (aka tryton-sao) before 7.6.9 allows XSS via an HTML attachment. This is fixed in 7.6.9, 7.4.19, 7.0.38, and 6.0.67.	5.4	More Details

CVE-2025-13157	The QODE Wishlist for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2.7 via the 'qode_wishlist_for_woocommerce_wishlist_table_item_callback' function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to update the public view of arbitrary wishlists.	5.3	More Details
CVE-2025-13441	The Hide Category by User Role for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.3.1. This is due to a missing capability check on the admin_init hook that executes wp_cache_flush(). This makes it possible for unauthenticated attackers to flush the site's object cache via forged requests, potentially degrading site performance.	5.3	More Details
CVE-2025-12584	The Quick View for WooCommerce plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.2.17 via the 'wqv_popup_content' AJAX endpoint due to insufficient restrictions on which products can be included. This makes it possible for unauthenticated attackers to extract data from private products that they should not have access to.	5.3	More Details
CVE-2025-20756	In Modem, there is a possible system crash due to a logic error. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01673749; Issue ID: MSV-4643.	5.3	More Details
CVE-2024-32388	Due to a firewall misconfiguration, Kerlink devices running KerOS prior to 5.12 incorrectly accept specially crafted UDP packets. This allows an attacker to bypass the firewall and access UDP-based services that would otherwise be protected.	5.3	More Details
CVE-2025-13696	The Zigaform plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 7.6.5. This is due to the plugin exposing a public AJAX endpoint that retrieves form submission data without performing authorization checks to verify ownership or access rights. This makes it possible for unauthenticated attackers to extract sensitive form submission data including personal information, payment details, and other private data via the rocket_front_payment_seesummary action by enumerating sequential form_r_id values.	5.3	More Details
CVE-2025-64313	Denial of service (DoS) vulnerability in the office service. Impact: Successful exploitation of this vulnerability may affect availability.	5.3	More Details
CVE-2025-12579	The Reuters Direct plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'logoff' action in all versions up to, and including, 3.0.0. This makes it possible for unauthenticated attackers to reset the plugin's settings.	5.3	More Details
CVE-2025-20792	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01717526; Issue ID: MSV-5591.	5.3	More Details
CVE-2025-20791	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01661189; Issue ID: MSV-4298.	5.3	More Details
CVE-2025-20790	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01677581; Issue ID: MSV-4701.	5.3	More Details
CVE-2025-13810	A vulnerability was found in jsnjfz WebStack-Guns 1.0. This affects the function renderPicture of the file src/main/java/com/jsnjfz/manage/modular/system/controller/KaptchaController.java. Performing manipulation results in path traversal. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for	5.3	More Details

20757	exploitation. Patch ID: MOLY01673751; Issue ID: MSV-4644.		
CVE-2025-59792	Reveals plaintext credentials in the MONITOR command vulnerability in Apache Kvrocks. This issue affects Apache Kvrocks: from 1.0.0 through 2.13.0. Users are recommended to upgrade to version 2.14.0, which fixes the issue.	5.3	More Details
CVE-2025-13876	A security vulnerability has been detected in Rareprob HD Video Player All Formats App 12.1.372 on Android. Impacted is an unknown function of the component com.rocks.music.videoplayer. The manipulation leads to path traversal. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-20755	In Modem, there is a possible application crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00628396; Issue ID: MSV-4775.	5.3	More Details
CVE-2025-20754	In Modem, there is a possible system crash due to an incorrect bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689251; Issue ID: MSV-4840.	5.3	More Details
CVE-2025-55181	Sending an HTTP request/response body with greater than 2^31 bytes triggers an infinite loop in proxygen::coro::HTTPQuicCoroSession which blocks the backing event loop and unconditionally appends data to a std::vector per-loop iteration. This issue leads to unbounded memory growth and eventually causes the process to run out of memory.	5.3	More Details
CVE-2025-20753	In Modem, there is a possible system crash due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01689252; Issue ID: MSV-4841.	5.3	More Details
CVE-2025-20751	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01661195; Issue ID: MSV-4297.	5.3	More Details
CVE-2025-20750	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01661199; Issue ID: MSV-4296.	5.3	More Details
CVE-2025-13381	The AI ChatBot with ChatGPT and Content Generator by AYS plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the 'ays_chatgpt_save_wp_media' function in all versions up to, and including, 2.7.0. This makes it possible for unauthenticated attackers to upload media files.	5.3	More Details
CVE-2025-57850	A container privilege escalation flaw was found in certain CodeReady Workspaces images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	5.2	More Details
CVE-2025-58312	Permission control vulnerability in the App Lock module. Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2025-2879	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU processing operations to expose sensitive data.This issue affects Valhall GPU Kernel Driver: from r29p0 through r49p4, from r50p0 through r54p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p4, from r50p0 through r54p0.	5.1	More Details
CVE-2025-	Permission control vulnerability in the Notepad module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.1	More Details

64311			
CVE-2025-6349	Use After Free vulnerability in Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU memory processing operations to gain access to already freed memory.This issue affects Valhall GPU Kernel Driver: from r53p0 through r54p1; Arm 5th Gen GPU Architecture Kernel Driver: from r53p0 through r54p1.	5.1	More Details
CVE-2025-58436	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. Prior to version 2.4.15, a client that connects to cupsd but sends slow messages, e.g. only one byte per second, delays cupsd as a whole, such that it becomes unusable by other clients. This issue has been patched in version 2.4.15.	5.1	More Details
CVE-2025-66432	In Oxide control plane 15 through 17 before 17.1, API tokens can be renewed past their expiration date.	5.0	More Details
CVE-2025-66370	Kivitendo before 3.9.2 allows XXE injection. By uploading an electronic invoice in the ZUGFeRD format, it is possible to read and exfiltrate files from the server's filesystem.	5.0	More Details
CVE-2025-66371	Peppol-py before 1.1.1 allows XXE attacks because of the Saxon configuration. When validating XML-based invoices, the XML parser could read files from the filesystem and expose their content to a remote host.	5.0	More Details
CVE-2025-58304	Permission control vulnerability in the file management module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.9	More Details
CVE-2025-64312	Permission control vulnerability in the file management module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.9	More Details
CVE-2025-66303	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, A Denial of Service (DoS) vulnerability has been identified in Grav related to the handling of scheduled_at parameters. Specifically, the application fails to properly sanitize input for cron expressions. By manipulating the scheduled_at parameter with a malicious input, such as a single quote, the application admin panel becomes non-functional, causing significant disruptions to administrative operations. The only way to recover from this issue is to manually access the host server and modify the backup.yaml file to correct the corrupted cron expression. This vulnerability is fixed in 1.8.0-beta.27.	4.9	More Details
CVE-2025-20758	In Modem, there is a possible system crash due to an uncaught exception. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01673755; Issue ID: MSV-4647.	4.9	More Details
CVE-2025-65955	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to 7.1.2-9 and 6.9.13-34, there is a vulnerability in ImageMagick's Magick++ layer that manifests when Options::fontFamily is invoked with an empty string. Clearing a font family calls RelinquishMagickMemory on _drawInfo->font, freeing the font string but leaving _drawInfo->font pointing to freed memory while _drawInfo->family is set to that (now-invalid) pointer. Any later cleanup or reuse of _drawInfo->font re-frees or dereferences dangling memory. DestroyDrawInfo and other setters (Options::font, Image::font) assume _drawInfo->font remains valid, so destruction or subsequent updates trigger crashes or heap corruption. This vulnerability is fixed in 7.1.2-9 and 6.9.13-34.	4.9	More Details
CVE-2025-12630	The Upload.am WordPress plugin before 1.0.1 is vulnerable to arbitrary option disclosure due to a missing capability check on its AJAX request handler, allowing users such as contributor to view site options.	4.9	More Details
CVE-2025-13090	The WP Directory Kit plugin for WordPress is vulnerable to SQL Injection via the 'search' parameter in all versions up to, and including, 1.4.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details

CVE-2025-13505	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting'), Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Datateam Information Technologies Inc. Datactive allows Stored XSS.This issue affects Datactive: from 2.13.34 before 2.14.0.6.	4.8	More Details
CVE-2025-20765	In aee daemon, there is a possible system crash due to a race condition. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10190802; Issue ID: MSV-4833.	4.7	More Details
CVE-2025-59302	In Apache CloudStack improper control of generation of code ('Code Injection') vulnerability is found in the following APIs which are accessible only to admins. * quotaTariffCreate * quotaTariffUpdate * createSecondaryStorageSelector * updateSecondaryStorageSelector * updateHost * updateStorage This issue affects Apache CloudStack: from 4.18.0 before 4.20.2, from 4.21.0 before 4.22.0. Users are recommended to upgrade to versions 4.20.2 or 4.22.0, which contain the fix. The fix introduces a new global configuration flag, js.interpretation.enabled, allowing administrators to control the interpretation of JavaScript expressions in these APIs, thereby mitigating the code injection risk.	4.7	More Details
CVE-2025-66403	FileRise is a self-hosted web-based file manager with multi-file upload, editing, and batch operations. Prior to 2.2.3, a stored cross-site scripting (XSS) vulnerability exists in the Filerise application due to improper handling of uploaded SVG files. The application accepts user-supplied SVG uploads without sanitizing or restricting embedded script content. When a malicious SVG containing inline JavaScript or event-based payloads is uploaded, it is later rendered directly in the browser whenever viewed within the application. Because SVGs are XML-based and allow scripting, they execute in the origin context of the application, enabling full stored XSS. This vulnerability is fixed in 2.2.3.	4.6	More Details
CVE-2025-63522	Reverse Tabnabbing vulnerability in FeehiCMS 2.1.1 in the Comments Management function	4.6	More Details
CVE-2025-64750	SingularityCE and SingularityPRO are open source container platforms. Prior to SingularityCE 4.3.5 and SingularityPRO 4.1.11 and 4.3.5, if a user relies on LSM restrictions to prevent malicious operations then, under certain circumstances, an attacker can redirect the LSM label write operation so that it is ineffective. The attacker must cause the user to run a malicious container image that redirects the mount of /proc to the destination of a shared mount, either known to be configured on the target system, or that will be specified by the user when running the container. The attacker must also control the content of the shared mount, for example through another malicious container which also binds it, or as a user with relevant permissions on the host system it is bound from. This vulnerability is fixed in SingularityCE 4.3.5 and SingularityPRO 4.1.11 and 4.3.5.	4.5	More Details
CVE-2025-65105	Apptainer is an open source container platform. In Apptainer versions less than 1.4.5, a container can disable two of the forms of the little used --security option, in particular the forms --security=apparmor:<profile> and --security=selinux:<label> which otherwise put restrictions on operations that containers can do. The --security option has always been mentioned in Apptainer documentation as being a feature for the root user, although these forms do also work for unprivileged users on systems where the corresponding feature is enabled. Apparmor is enabled by default on Debian-based distributions and SElinux is enabled by default on RHEL-based distributions, but on SUSE it depends on the distribution version. This vulnerability is fixed in 1.4.5.	4.5	More Details
CVE-2025-58488	Improper verification of source of a communication channel in SmartTouchCall prior to version 1.0.1.1 allows remote attackers to access sensitive information. User interaction is required for triggering this vulnerability.	4.5	More Details
CVE-2025-64315	Configuration defect vulnerability in the file management module. Impact: Successful exploitation of this vulnerability may affect app data confidentiality and integrity.	4.4	More Details
CVE-2025-13635	Inappropriate implementation in Downloads in Google Chrome prior to 143.0.7499.41 allowed a local attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.4	More Details
CVE-2025-	In GPU pdma, there is a possible memory corruption due to a missing permission check. This could lead to local denial of service with no additional execution privileges needed. User	4.4	More

20788	interaction is needed for exploitation. Patch ID: ALPS10117735; Issue ID: MSV-4539.		Details
CVE-2025-20789	In GPU pdma, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS10117741; Issue ID: MSV-4538.	4.4	More Details
CVE-2025-12185	The StaffList plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-13634	Inappropriate implementation in Downloads in Google Chrome on Windows prior to 143.0.7499.41 allowed a local attacker to bypass mark of the web via a crafted HTML page. (Chromium security severity: Medium)	4.4	More Details
CVE-2025-12971	The Folders – Unlimited Folders to Organize Media Library Folder, Pages, Posts, File Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a misconfigured capability check on the 'wcp_change_post_folder' function in all versions up to, and including, 3.1.5. This makes it possible for authenticated attackers, with Contributor-level access and above, to move arbitrary folder contents to arbitrary folders.	4.3	More Details
CVE-2025-65670	An Insecure Direct Object Reference (IDOR) in classroomio 0.1.13 allows students to access sensitive admin/teacher endpoints by manipulating course IDs in URLs, resulting in unauthorized disclosure of sensitive course, admin, and student data. The leak occurs momentarily before the system reverts to a normal state restricting access.	4.3	More Details
CVE-2025-13807	A vulnerability was detected in orionsec orion-ops up to 5925824997a3109651bbde07460958a7be249ed1. Affected is the function MachineKeyController of the file orion-ops-api/orion-ops-web/src/main/java/cn/orionsec/ops/controller/MachineKeyController.java of the component API. The manipulation results in improper authorization. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-58477	Out-of-bounds write in parsing IFD tag in libimagecodec.quram.so prior to SMR Dec-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-12756	Mattermost versions 11.0.x <= 11.0.2, 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12 fail to validate user permissions when deleting comments in Boards, which allows an authenticated user with the editor role to delete comments created by other users.	4.3	More Details
CVE-2025-13793	A weakness has been identified in winston-dsouza Ecommerce-Website up to 87734c043269baac0b4cfe9664784462138b1b2e. Affected by this issue is some unknown functionality of the file /includes/header_menu.php of the component GET Parameter Handler. Executing manipulation of the argument Error can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be exploited. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-66025	Caido is a web security auditing toolkit. Prior to version 0.53.0, the Markdown renderer used in Caido's Findings page improperly handled user-supplied Markdown, allowing attacker-controlled links to be rendered without confirmation. When a user opened a finding generated through the scanner, or other plugins, clicking these injected links could redirect the Caido application to an attacker-controlled domain, enabling phishing style attacks. This issue has been patched in version 0.53.0.	4.3	More Details
CVE-2025-13802	A vulnerability was determined in jairiidriss RestaurantWebsite up to e7911f12d035e8e2f9a75e7a28b59e4ef5c1d654. Impacted is an unknown function of the component Make a Reservation. This manipulation of the argument selected_date causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Continious delivery with rolling releases is used by this product. Therefore, no	4.3	More Details

	version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-13804	A security flaw has been discovered in nutzam NutzBoot up to 2.6.0-SNAPSHOT. The impacted element is an unknown function of the file nutzboot-demo/nutzboot-demo-simple/nutzboot-demo-simple-web3j/src/main/java/io/nutz/demo/simple/module/EthModule.java of the component Ethereum Wallet Handler. Performing manipulation results in information disclosure. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-65239	Incorrect access control in the /aux1/ocussd/trace endpoint of OpenCode Systems USSD Gateway OC Release:5, version 6.13.11 allows attackers with low-level privileges to read server logs.	4.3	More Details
CVE-2025-58478	Out-of-bounds write in libimagecodec.quram.so prior to SMR Dec-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-66306	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, there is an IDOR (Insecure Direct Object Reference) vulnerability in the Grav CMS Admin Panel which allows low-privilege users to access sensitive information from other accounts. Although direct account takeover is not possible, admin email addresses and other metadata can be exposed, increasing the risk of phishing, credential stuffing, and social engineering. This vulnerability is fixed in 1.8.0-beta.27.	4.3	More Details
CVE-2025-10476	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpfc_db_fix_callback() function in all versions up to, and including, 1.4.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to initiate several database fix actions. This only affects sites with premium activated.	4.3	More Details
CVE-2025-58479	Out-of-bounds read in libimagecodec.quram.so prior to SMR Dec-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-12559	Mattermost versions 11.0.x <= 11.0.2, 10.12.x <= 10.12.1, 10.11.x <= 10.11.4, 10.5.x <= 10.5.12 fail to sanitize team email addresses to be visible only to Team Admins, which allows any authenticated user to view team email addresses via the GET /api/v4/channels/{channel_id}/common_teams endpoint	4.3	More Details
CVE-2025-58480	Heap-based buffer overflow in libimagecodec.quram.so prior to SMR Dec-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-13143	The Poll, Survey & Quiz Maker Plugin by Opinion Stage plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 19.12.0. This is due to missing or insufficient nonce validation on the disconnect_account_action function. This makes it possible for unauthenticated attackers to disconnect the site from the Opinion Stage platform integration via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-59454	In Apache CloudStack, a gap in access control checks affected the APIs - createNetworkACL - listNetworkACLs - listResourceDetails - listVirtualMachinesUsageHistory - listVolumesUsageHistory While these APIs were accessible only to authorized users, insufficient permission validation meant that users could occasionally access information beyond their intended scope. Users are recommended to upgrade to Apache CloudStack 4.20.2.0 or 4.22.0.0, which fixes the issue.	4.3	More Details
CVE-2025-6195	GitLab has remediated an issue in GitLab EE affecting all versions from 13.7 before 18.4.5, 18.5 before 18.5.3, and 18.6 before 18.6.1 that could have allowed an authenticated user to view information from security reports under certain configuration conditions.	4.3	More Details
CVE-2025-13785	A security vulnerability has been detected in yungifez Skuul School Management System up to 2.6.5. This issue affects some unknown processing of the file /user/profile of the component Image Handler. Such manipulation leads to information disclosure. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
	An issue was discovered in 5.2 before 5.2.9, 5.1 before 5.1.15, and 4.2 before 4.2.27.		

CVE-2025-13372	`FilteredRelation` is subject to SQL injection in column aliases, using a suitably crafted dictionary, with dictionary expansion, as the `**kwargs` passed to `QuerySet.annotate()` or `QuerySet.alias()` on PostgreSQL. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Stackered for reporting this issue.	4.3	More Details
CVE-2025-66422	Tryton trytond before 7.6.11 allows remote attackers to obtain sensitive trace-back (server setup) information. This is fixed in 7.6.11, 7.4.21, 7.0.40, and 6.0.70.	4.3	More Details
CVE-2025-13129	Improper Enforcement of Behavioral Workflow vulnerability in Seneka Software Hardware Information Technology Trade Contracting and Industry Ltd. Co. Onaylarım allows Functionality Misuse.This issue affects Onaylarım: from 25.09.26.01 through 18112025.	4.3	More Details
CVE-2025-13765	Exposure of email service credentials to users without administrative rights in Devolutions Server.This issue affects Devolutions Server: before 2025.2.21, before 2025.3.9.	4.3	More Details
CVE-2025-11726	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.9.4. This is due to insufficient capability checks in the REST API endpoints under the 'fl-controls/v1' namespace that control site-wide Global Presets. This makes it possible for authenticated attackers with contributor-level access and above to add, modify, or delete global color and background presets that affect all Beaver Builder content site-wide.	4.3	More Details
CVE-2025-13685	The Photo Gallery by Ays plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.4.8. This is due to missing nonce verification on the bulk action functionality in the 'process_bulk_action()' function. This makes it possible for unauthenticated attackers to perform bulk operations (delete, publish, or unpublish galleries) via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13140	The SurveyJS: Drag & Drop WordPress Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12.20. This is due to missing nonce validation on the SurveyJS_DeleteSurvey AJAX action. This makes it possible for unauthenticated attackers to delete surveys via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13790	A vulnerability was determined in Scada-LTS up to 2.7.8.1. This impacts an unknown function. This manipulation causes cross-site request forgery. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-12578	The Reuters Direct plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation on the the 'class-reuters-direct-settings.php' page. This makes it possible for unauthenticated attackers to reset the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13637	Inappropriate implementation in Downloads in Google Chrome prior to 143.0.7499.41 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass download protections via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2025-13653	In Search Guard FLX versions from 3.1.0 up to 4.0.0 with enterprise modules being disabled, there exists an issue which allows authenticated users to use specially crafted requests to read documents from data streams without having the respective privileges.	4.3	More Details
CVE-2025-13636	Inappropriate implementation in Split View in Google Chrome prior to 143.0.7499.41 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted domain name. (Chromium security severity: Low)	4.3	More Details
CVE-2025-13737	The Nextend Social Login and Register plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.21. This is due to missing or incorrect nonce validation on the 'unlinkUser' function. This makes it possible for unauthenticated attackers to unlink the user's social login via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE-2025-58476	Out-of-bounds read vulnerability in bootloader prior to SMR Dec-2025 Release 1 allows physical attackers to access out-of-bounds memory.	4.2	More Details
CVE-2025-66433	HTCondor Access Point before 25.3.1 allows an authenticated user to impersonate other users on the local machine by submitting a batch job. This is fixed in 24.12.14, 25.0.3, and 25.3.1. The earliest affected version is 24.7.3.	4.2	More Details
CVE-2025-66386	app/Model/EventReport.php in MISP before 2.5.27 allows path traversal in view picture for a site-admin.	4.1	More Details
CVE-2025-13001	The donation WordPress plugin through 1.0 does not sanitize and escape a parameter before using it in a SQL statement, allowing high privilege users, such as admin to perform SQL injection attacks	4.1	More Details
CVE-2025-59701	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a physically proximate attacker (with elevated privileges) to read and modify the Appliance SSD contents (because they are unencrypted).	4.1	More Details
CVE-2025-58486	Improper input validation in Samsung Account prior to version 15.5.01.1 allows local attacker to execute arbitrary script.	4.0	More Details
CVE-2025-41743	Insufficient encryption strength in Sprecher Automation SPRECON-E-C, SPRECON-E-P, and SPRECON-E-T3 allows a local unprivileged attacker to extract data from update images and thus obtain limited information about the architecture and internal processes.	4.0	More Details
CVE-2025-58484	Incorrect default permissions in Samsung Cloud Assistant prior to version 8.0.03.8 allows local attacker to access partial data in sandbox.	4.0	More Details
CVE-2025-64715	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.16.17, 1.17.10, and 1.18.4, CiliumNetworkPolicys which use egress.toGroups.aws.securityGroupsIds to reference AWS security group IDs that do not exist or are not attached to any network interface may unintentionally allow broader outbound access than intended by the policy authors. In such cases, the toCIDRset section of the derived policy is not generated, which means outbound traffic may be permitted to more destinations than originally intended. This issue has been patched in versions 1.16.17, 1.17.10, and 1.18.4. There are no workarounds for this issue.	4.0	More Details
CVE-2025-58487	Improper authorization in Samsung Account prior to version 15.5.01.1 allows local attacker to launch arbitrary activity with Samsung Account privilege.	4.0	More Details
CVE-2025-8045	Use After Free vulnerability in Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU processing operations to gain access to already freed memory.This issue affects Valhall GPU Kernel Driver: from r53p0 through r54p1; Arm 5th Gen GPU Architecture Kernel Driver: from r53p0 through r54p1.	4.0	More Details
CVE-2025-13805	A weakness has been identified in nutzam NutzBoot up to 2.6.0-SNAPSHOT. This affects the function getInputStream of the file nutzcloud/nutzcloud-literpc/src/main/java/org/nutz/boot/starter/literpc/impl/endpoint/http/HttpServletRpcEndpoint.java of the component LiteRpc-Serializer. Executing manipulation can lead to deserialization. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is reported as difficult. The exploit has been made available to the public and could be exploited.	3.7	More Details
CVE-2025-66040	Spotipy is a Python library for the Spotify Web API. Prior to version 2.25.2, there is a cross-site scripting (XSS) vulnerability in the OAuth callback server that allows for JavaScript injection through the unsanitized error parameter. Attackers can execute arbitrary JavaScript in the user's browser during OAuth authentication. This issue has been patched in version 2.25.2.	3.6	More Details
CVE-2025-65858	A Stored Cross-Site Scripting (XSS) vulnerability in Calibre-Web v0.6.25 allows attackers to inject malicious JavaScript into the 'username' field during user creation. The payload is stored unsanitized and later executed when the /ajax/listusers endpoint is accessed.	3.5	More Details

CVE-2025-13758	Exposure of credentials in unintended requests in Devolutions Server.This issue affects Server: through 2025.2.20, through 2025.3.8.	3.5	More Details
CVE-2025-13640	Inappropriate implementation in Passwords in Google Chrome prior to 143.0.7499.41 allowed a local attacker to bypass authentication via physical access to the device. (Chromium security severity: Low)	3.5	More Details
CVE-2025-20769	In display, 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: ALPS10196993; Issue ID: MSV-4804.	3.4	More Details
CVE-2025-65681	An issue was discovered in Overhang.IO (tutor-open-edx) (overhangio/tutor) 20.0.2 allowing local unauthorized attackers to gain access to sensitive information due to the absence of proper cache-control HTTP headers and client-side session checks.	3.3	More Details
CVE-2025-55174	In KDE Skanpage before 25.08.0, an attempt at file overwrite can result in the contents of the new file at the beginning followed by the partial contents of the old file at the end, because of use of QIODevice::ReadWrite instead of QODevice::WriteOnly.	3.2	More Details
CVE-2025-59696	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a physically proximate attacker to modify or erase tamper events via the Chassis management board.	3.2	More Details
CVE-2025-13870	Mattermost versions 10.11.x <= 10.11.4, 10.5.x <= 10.5.12 fail to validate the user permission when accessing the files and subscribing to the block in Boards, which allows an authenticated user to access other board files and was able to subscribe to the block from other boards that the user does not have access to	3.1	More Details
CVE-2025-66382	In libexpat through 2.7.3, a crafted file with an approximate size of 2 MiB can lead to dozens of seconds of processing time.	2.9	More Details
CVE-2025-66372	Mustang before 2.16.3 allows exfiltrating files via XXE attacks.	2.8	More Details
CVE-2025-20373	In Splunk Add-on for Palo Alto Networks versions below 2.0.2, the add-on exposes client secrets in plain text in the _internal index during the addition of new “Data Security Accounts“. The vulnerability would require either local access to the log files or administrative access to internal indexes, which by default only the admin role receives. Review roles and capabilities on your instance and restrict internal index access to administrator-level roles. See [Define roles on the Splunk platform with capabilities] (https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities) in the Splunk documentation for more information.	2.7	More Details
CVE-2025-13784	A weakness has been identified in yungifez Skuul School Management System up to 2.6.5. This vulnerability affects unknown code of the file /dashboard/schools/1/edit of the component SVG File Handler. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-13795	A weakness has been identified in codingWithElias School Management System up to f1ac334bfd89ae9067cc14dea12ec6ff3f078c01. Affected is an unknown function of the file /student-view.php of the component Edit Student Info Page. This manipulation of the argument First Name causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-6666	A vulnerability was determined in motogadget mo.lock Ignition Lock up to 20251125. Affected by this vulnerability is an unknown functionality of the component NFC Handler. Executing manipulation can lead to use of hard-coded cryptographic key . The physical device can be targeted for the attack. A high complexity level is associated with this attack. The exploitation	2.0	More Details

	appears to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-13611	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.2 before 18.4.5, 18.5 before 18.5.3, and 18.6 before 18.6.1 that could have allowed an authenticated user with access to certain logs to obtain sensitive tokens under specific conditions.	2.0	More Details
CVE-2025-65957	Core Bot Is an Open Source discord bot made for maple hospital servers. Prior to commit dffe050, the API keys (SUPABASE_API_KEY, TOKEN) are loaded using environment variables, but there are cases in code (error handling, summaries, webhooks) where configuration summaries may inadvertently leak sensitive data (e.g., by failing to redact data in summary embeds or logs). This issue has been patched via commit dffe050.	N/A	More Details
CVE-2025-66360	An issue was discovered in Logpoint before 7.7.0. An improperly configured access control policy exposes sensitive Logpoint internal service (Redis) information to li-admin users. This can lead to privilege escalation.	N/A	More Details
CVE-2025-66361	An issue was discovered in Logpoint before 7.7.0. Sensitive information is exposed in System Processes for an extended period during high CPU load.	N/A	More Details
CVE-2025-66266	The RupsMon.exe service executable in UPSilon 2000 has insecure permissions, allowing the 'Everyone' group Full Control. A local attacker can replace the executable with a malicious binary to execute code with SYSTEM privileges or simply change the config path of the service to a command; starting and stopping the service to immediately achieve code execution and privilege escalation	N/A	More Details
CVE-2025-59703	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a Physically Proximate Attacker to access the internal components of the appliance, without leaving tamper evidence. To exploit this, the attacker needs to remove the tamper label and all fixing screws from the device without damaging it. This is called an F14 attack.	N/A	More Details
CVE-2025-59704	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow an attacker to gain access the the BIOS menu because is has no password.	N/A	More Details
CVE-2025-41012	Unauthorized access vulnerability in TCMAN GIM v11 version 20250304. This vulnerability allows an unauthenticated attacker to determine whether a user exists on the system by using the 'pda:userId' and 'pda:newPassword' parameters with 'soapaction UnlockUser’ in '/WS/PDAWebService.asmx'.	N/A	More Details
CVE-2025-66021	OWASP Java HTML Sanitizer is a configureable HTML Sanitizer written in Java, allowing inclusion of HTML authored by third-parties in web applications while protecting against XSS. In version 20240325.1, OWASP java html sanitizer is vulnerable to XSS if HtmlPolicyBuilder allows noscript and style tags with allowTextIn inside the style tag. This could lead to XSS if the payload is crafted in such a way that it does not sanitise the CSS and allows tags which is not mentioned in HTML policy. At time of publication no known patch is available.	N/A	More Details
CVE-2025-13827	Summary Arbitrary files can be uploaded via the GrapesJS Builder, as the types of files that can be uploaded are not restricted. ImpactIf the media folder is not restricted from running files this can lead to a remote code execution.	N/A	More Details
CVE-2025-41013	SQL injection vulnerability in TCMAN GIM v11 in version 20250304. This vulnerability allows an attacker to retrieve, create, update, and delete databases by sending a GET request using the 'idmant' parameter in '/PC/frmEPIS.aspx'.	N/A	More Details
CVE-2025-13828	SummaryA non privileged user can install and remove arbitrary packages via composer for a composer based installed, even if the flag in update settings for enable composer based update is unticked. ImpactA low-privileged user of the platform can install malicious code to obtain higher privileges.	N/A	More Details
CVE-2025-	OrangeHRM is a comprehensive human resource management (HRM) system. From version 5.0 to 5.7, the interview attachment retrieval endpoint in the Recruitment module serves files based solely on an authenticated session and user-supplied identifiers, without verifying whether the requester has permission to access the associated interview record. Because the server does not perform any recruitment-level authorization checks, an ESS-level user with no access to	N/A	More

66291	recruitment workflows can directly request interview attachment URLs and receive the corresponding files. This exposes confidential interview documents—including candidate CVs, evaluations, and supporting files—to unauthorized users. The issue arises from relying on predictable object identifiers and session presence rather than validating the user's association with the relevant recruitment process. This issue has been patched in version 5.8.		Details
CVE-2025-66290	OrangeHRM is a comprehensive human resource management (HRM) system. From version 5.0 to 5.7, the application's recruitment attachment retrieval endpoint does not enforce the required authorization checks before serving candidate files. Even users restricted to ESS-level access, who have no permission to view the Recruitment module, can directly access candidate attachment URLs. When an authenticated request is made to the attachment endpoint, the system validates the session but does not confirm that the requesting user has the necessary recruitment permissions. As a result, any authenticated user can download CVs and other uploaded documents for arbitrary candidates by issuing direct requests to the attachment endpoint, leading to unauthorized exposure of sensitive applicant data. This issue has been patched in version 5.8.	N/A	More Details
CVE-2025-65358	Edoc-doctor-appointment-system v1.0.1 was discovered to contain SQl injection vulnerability via the 'docid' parameter at /admin/appointment.php.	N/A	More Details
CVE-2025-65656	dcat-admin v2.2.3-beta and before is vulnerable to file inclusion in admin/src/Extend/VersionManager.php.	N/A	More Details
CVE-2025-66289	OrangeHRM is a comprehensive human resource management (HRM) system. From version 5.0 to 5.7, the application does not invalidate existing sessions when a user is disabled or when a password change occurs, allowing active session cookies to remain valid indefinitely. As a result, a disabled user, or an attacker using a compromised account, can continue to access protected pages and perform operations as long as a prior session remains active. Because the server performs no session revocation or session-store cleanup during these critical state changes, disabling an account or updating credentials has no effect on already-established sessions. This makes administrative disable actions ineffective and allows unauthorized users to retain full access even after an account is closed or a password is reset, exposing the system to prolonged unauthorized use and significantly increasing the impact of account takeover scenarios. This issue has been patched in version 5.8.	N/A	More Details
CVE-2025-58386	In Terminalfour 8 through 8.4.1.1, the userLevel parameter in the user management function is not subject to proper server-side authorization checks. A Power User can intercept and modify this parameter to assign the Administrator role to other existing lower-privileged accounts, or invite a new lower-privileged account and escalate its privileges. While manipulating this request, the Power User can also change the target account's password, effectively taking full control of it.	N/A	More Details
CVE-2025-60854	A vulnerability has been found in D-Link R15 (AX1500) 1.20.01 and below. By manipulating the model name parameter during a password change request in the web administrator page, it is possible to trigger a command injection in httpd.	N/A	More Details
CVE-2025-13338	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-59705	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a Physically Proximate Attacker to Escalate Privileges by enabling the USB interface through chassis probe insertion during system boot, aka "Unauthorized Reactivation of the USB interface" or F01.	N/A	More Details
CVE-2025-66269	The RupsMon and USBMate services in UPSilon 2000 run with SYSTEM privileges and contain unquoted service paths. This allows a local attacker to perform path interception and escalate privileges if they have write permissions to the directories proceeding that of which the real service executables live in	N/A	More Details
	OrangeHRM is a comprehensive human resource management (HRM) system. From version 5.0 to 5.7, the application contains an input-neutralization flaw in its mail configuration and delivery workflow that allows user-controlled values to flow directly into the system's sendmail command. Because these values are not sanitized or constrained before being incorporated into the		

CVE-2025-66224	command execution path, certain sendmail behaviors can be unintentionally invoked during email processing. This makes it possible for the application to write files on the server as part of the mail-handling routine, and in deployments where those files end up in web-accessible locations, the behavior can be leveraged to achieve execution of attacker-controlled content. The issue stems entirely from constructing OS-level command strings using unsanitized input within the mail-sending logic. This issue has been patched in version 5.8.	N/A	More Details
CVE-2025-41014	User Enumeration Vulnerability in TCMAN GIM v11 version 20250304. This vulnerability allows an unauthenticated attacker to determine whether a user exists on the system. The vulnerability is exploitable through the 'pda:username' parameter with 'soapaction GetLastDatePasswordChange' in '/WS/PDAWebService.asmx'.	N/A	More Details
CVE-2025-41015	User Enumeration Vulnerability in TCMAN GIM v11 version 20250304. This vulnerability allows an unauthenticated attacker to determine whether a user exists on the system. The vulnerability is exploitable through the 'pda:username' parameter with 'soapaction GetUserQuestionAndAnswer' in '/WS/PDAWebService.asmx'.	N/A	More Details
CVE-2025-41066	Horde Groupware v5.2.22 has a user enumeration vulnerability that allows an unauthenticated attacker to determine the existence of valid accounts on the system. To exploit the vulnerability, an HTTP request must be sent to ‘/imp/attachment.php’ including the parameters ‘id’ and ‘u’. If the specified user exists, the server will return the download of an empty file; if it does not exist, no download will be initiated, which unequivocally reveals the validity of the user.	N/A	More Details
CVE-2025-41086	Vulnerability in the access control system of the GAMS licensing system that allows unlimited valid licenses to be generated, bypassing any usage restrictions. The validator uses an insecure checksum algorithm; knowing this algorithm and the format of the license lines, an attacker can recalculate the checksum and generate a valid license to grant themselves full privileges without credentials or access to the source code, allowing them unrestricted access to GAMS's mathematical models and commercial solvers.	N/A	More Details
CVE-2025-41070	Reflected Cross-site Scripting (XSS) vulnerability in Sanoma's Clickedu. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending them a malicious URL in '/students/carpetes_varies.php'. This vulnerability can be exploited to steal sensitive user data, such as session cookies, or to perform actions on behalf of the user.	N/A	More Details
CVE-2025-13742	Emails sent by pretix can utilize placeholders that will be filled with customer data. For example, when {name} is used in an email template, it will be replaced with the buyer's name for the final email. If the name of the attendee contained HTML or Markdown formatting, this was rendered as HTML in the resulting email. This way, a user could inject links or other formatted text through a maliciously formatted name. Since pretix applies a strict allow list approach to allowed HTML tags, this could not be abused for XSS or similarly dangerous attack chains. However, it can be used to manipulate emails in a way that makes user-provided content appear in a trustworthy and credible way, which can be abused for phishing.	N/A	More Details
CVE-2025-12140	The application contains an insecure 'redirectToUrl' mechanism that incorrectly processes the value of the 'redirectUrlParameter' parameter. The application interprets the entered string of characters as a Java expression, allowing an unauthenticated attacer to perform arbitrary code execution. This issue was fixed in version wu#2016.1.5513#0#20251014_113353	N/A	More Details
CVE-2025-27232	An authenticated Zabbix Super Admin can exploit the oauth.authorize action to read arbitrary files from the webserver leading to potential confidentiality loss.	N/A	More Details
CVE-2025-8890	Firmware in SDMC NE6037 routers prior to version 7.1.12.2.44 has a network diagnostics tool vulnerable to a shell command injection attacks. In order to exploit this vulnerability, an attacker has to log in to the router's administrative portal, which by default is reachable only via LAN ports.	N/A	More Details
CVE-2025-59693	The Chassis Management Board in Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allows a physically proximate attacker to obtain debug access and escalate privileges by bypassing the tamper label and opening the chassis without leaving evidence, and accessing the JTAG connector. This is called F02.	N/A	More Details
CVE-2025-	The Chassis Management Board in Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allows a physically proximate attacker to persistently modify firmware and influence the (insecurely configured) appliance boot process. To exploit this, the attacker	N/A	More

59694	must modify the firmware via JTAG or perform an upgrade to the chassis management board firmware. This is called F03.		Details
CVE-2025-59695	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a user with OS root access to alter firmware on the Chassis Management Board (without Authentication). This is called F04.	N/A	More Details
CVE-2025-3261	ThingsBoard in versions prior to v4.2.1 allows an authenticated user to upload malicious SVG images via the "Image Gallery", leading to a Stored Cross-Site Scripting (XSS) vulnerability. The exploit can be triggered when any user accesses the public API endpoint of the malicious SVG images, or if the malicious images are embedded in an `iframe` element, during a widget creation, deployed to any page of the platform (e.g., dashboards), and accessed during normal operations. The vulnerability resides in the `ImageController`, which fails to restrict the execution of JavaScript code when an image is loaded by the user's browser. This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions.	N/A	More Details
CVE-2025-64772	The installer of INZONE Hub 1.0.10.3 to 1.0.17.0 contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with the privilege of the user invoking the installer.	N/A	More Details
CVE-2025-59698	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, might allow a physically proximate attacker to gain access to the EOL legacy bootloader.	N/A	More Details
CVE-2025-59699	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a physically proximate attacker to escalate privileges by booting from a USB device with a valid root filesystem. This occurs because of insecure default settings in the Legacy GRUB Bootloader.	N/A	More Details
CVE-2025-59700	Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7, allow a physically proximate attacker with root access to modify the Recovery Partition (because of a lack of integrity protection).	N/A	More Details
CVE-2025-66225	OrangeHRM is a comprehensive human resource management (HRM) system. From version 5.0 to 5.7, the password reset workflow does not enforce that the username submitted in the final reset request matches the account for which the reset process was originally initiated. After obtaining a valid reset link for any account they can receive email for, an attacker can alter the username parameter in the final reset request to target a different user. Because the system accepts the supplied username without verification, the attacker can set a new password for any chosen account, including privileged accounts, resulting in full account takeover. This issue has been patched in version 5.8.	N/A	More Details
CVE-2025-65844	EverShop 2.0.1 allows an unauthenticated user to upload files and create directories within the /api/images endpoint.	N/A	More Details
CVE-2025-66223	OpenObserve is a cloud-native observability platform. Prior to version 0.16.0, organization invitation tokens do not expire once issued, remain valid even after the invited user is removed from the organization, and allow multiple invitations to the same email with different roles where all issued links remain valid simultaneously. This results in broken access control where a removed or demoted user can regain access or escalate privileges. This issue has been patched in version 0.16.0.	N/A	More Details
CVE-2025-13879	Directory traversal vulnerability in SOLIDserver IPAM v8.2.3. This vulnerability allows an authenticated user with administrator privileges to list directories other than those to which the have authorized access using the 'directory' parameter in '/mod/ajax.php?action=sections/list/list'.For examplem setting the 'directory' parameter to '/' displays files outside the 'LOCAL:///' folder.	N/A	More Details
CVE-2025-66416	The MCP Python SDK, called `mcp` on PyPI, is a Python implementation of the Model Context Protocol (MCP). Prior to version 1.23.0, tThe Model Context Protocol (MCP) Python SDK does not enable DNS rebinding protection by default for HTTP-based servers. When an HTTP-based MCP server is run on localhost without authentication using FastMCP with streamable HTTP or SSE transport, and has not configured TransportSecuritySettings, a malicious website could exploit DNS rebinding to bypass same-origin policy restrictions and send requests to the local MCP server. This could allow an attacker to invoke tools or access resources exposed by the MCP	N/A	More Details

	server on behalf of the user in those limited circumstances. Note that running HTTP-based MCP servers locally without authentication is not recommended per MCP security best practices. This issue does not affect servers using stdio transport. This vulnerability is fixed in 1.23.0.		
CVE-2025-66259	Authenticated Root Remote Code Execution via improrer user input filtering in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform in main_ok.php user supplied data/hour/time is passed directly into date shell command	N/A	More Details
CVE-2025-66458	Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other. Prior to 1.35.3, there are multiple XSS due to unsafe use of f-strings in Markup. The issue requires a malicious 3rd party server responding with a JSON document containing JS code in a script element. This vulnerability is fixed in 1.35.3.	N/A	More Details
CVE-2025-66459	Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other. Prior to 1.35.3, a XSS vulnerability can be triggered when a user submits a list of URLs to capture, one of them contains a HTML element, and the capture fails. Then, the error field is populated with an error message that contains the bad URL they tried to capture, triggering the XSS. This vulnerability is fixed in 1.35.3.	N/A	More Details
CVE-2025-66460	Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other. Prior to 1.35.3, Lookyloo passed improperly escaped values to cells rendered in datatables using the orthogonal-data feature. It is definitely exploitable from the popup view, but it is most probably also exploitable in many other places. This vulnerability is fixed in 1.35.3.	N/A	More Details
CVE-2025-66258	Stored Cross-Site Scripting via XML Injection in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Stored XSS via crafted filenames injected into patchlist.xml. User-controlled filenames are directly concatenated into `patchlist.xml` without encoding, allowing injection of malicious JavaScript payloads via crafted filenames (e.g., `<img src=x onerror=alert()>.bin`). The XSS executes when ajax.js processes and renders the XML file.	N/A	More Details
CVE-2025-13510	The Iskra iHUB and iHUB Lite smart metering gateway exposes its web management interface without requiring authentication, allowing unauthenticated users to access and modify critical device settings.	N/A	More Details
CVE-2025-13658	A vulnerability in Longwatch devices allows unauthenticated HTTP GET requests to execute arbitrary code via an exposed endpoint, due to the absence of code signing and execution controls. Exploitation results in SYSTEM-level privileges.	N/A	More Details
CVE-2025-66257	Unauthenticated Arbitrary File Deletion (patch_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform The deletepatch parameter allows unauthenticated deletion of arbitrary files. The `deletepatch` parameter in `patch_contents.php` allows unauthenticated deletion of arbitrary files in `/var/www/patch/` directory without sanitization or access control checks.	N/A	More Details
CVE-2025-66256	Unauthenticated Arbitrary File Upload (patch_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Unrestricted file upload in patch_contents.php allows uploading malicious files. The `/var/tdf/patch_contents.php` endpoint allows unauthenticated arbitrary file uploads without file type validation, MIME checking, or size restrictions beyond 16MB, enabling attackers to upload malicious files.	N/A	More Details
CVE-2025-66255	Unauthenticated Arbitrary File Upload (upgrade_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Missing signature validation allows uploading malicious firmware packages. The firmware upgrade endpoint in `upgrade_contents.php` accepts arbitrary file uploads without validating file headers, cryptographic signatures, or enforcing .tgz format requirements, allowing malicious firmware injection. This endpoint also subsequently provides ways for arbitrary file uploads and subsequent remote code execution	N/A	More Details
	Unauthenticated Arbitrary File Deletion (upgrade_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000,		

CVE-2025-66254	3000, 3500, 6000, 7000 allows an attacker to perform The deleteupgrade parameter allows unauthenticated deletion of arbitrary files. The `deleteupgrade` parameter in `/var/www/upgrade_contents.php` allows unauthenticated deletion of arbitrary files in `/var/www/upload/` without any extension restriction or path sanitization, enabling attackers to remove critical system files.	N/A	More Details
CVE-2025-66253	Unauthenticated OS Command Injection (start_upgrade.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform User input passed directly to exec() allows remote code execution via start_upgrade.php. The `/var/tdf/start_upgrade.php` endpoint passes user-controlled `$_GET["filename"]` directly into `exec()` without sanitization or shell escaping. Attackers can inject arbitrary shell commands using metacharacters (`;`, `|`, etc.) to achieve remote code execution as the web server user (likely root).	N/A	More Details
CVE-2025-66252	Infinite Loop Denial of Service via Failed File Deletion in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Infinite loop when unlink() fails in status_contents.php causing DoS. Due to the fact that the unlink operation is done in a while loop; if an immutable file is specified or otherwise a file in which the process has no permissions to delete; it would repeatedly attempt to do in a loop.	N/A	More Details
CVE-2025-66251	Unauthenticated Path Traversal with Arbitrary File Deletion in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform The deletehidden parameter allows path traversal deletion of arbitrary .tgz files.	N/A	More Details
CVE-2025-66250	Unauthenticated Arbitrary File Upload (status_contents.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Allows unauthenticated arbitrary file upload via /var/tdf/status_contents.php.	N/A	More Details
CVE-2025-66019	pypdf is a free and open-source pure-python PDF library. Prior to version 6.4.0, an attacker who uses this vulnerability can craft a PDF which leads to a memory usage of up to 1 GB per stream. This requires parsing the content stream of a page using the LZWDecode filter. This issue has been patched in version 6.4.0.	N/A	More Details
CVE-2025-11156	Netskope was notified about a potential gap in its agent (NS Client) on Windows systems. If this gap is successfully exploited, a local, authenticated user with Administrator privileges can improperly load the driver as a generic kernel service. This triggers the flaw, causing a system crash (Blue-Screen-of-Death) and resulting in a Denial of Service (DoS) for the affected machine.	N/A	More Details
CVE-2025-66385	UsersController::edit in Cerebrate before 1.30 allows an authenticated non-privileged user to escalate their privileges (e.g., obtain a higher role such as admin) via the user-edit endpoint by supplying or modifying role_id or organisation_id fields in the edit request.	N/A	More Details
CVE-2025-66414	MCP TypeScript SDK is the official TypeScript SDK for Model Context Protocol servers and clients. Prior to 1.24.0, The Model Context Protocol (MCP) TypeScript SDK does not enable DNS rebinding protection by default for HTTP-based servers. When an HTTP-based MCP server is run on localhost without authentication with StreamableHTTPServerTransport or SSEServerTransport and has not enabled enableDnsRebindingProtection, a malicious website could exploit DNS rebinding to bypass same-origin policy restrictions and send requests to the local MCP server. This could allow an attacker to invoke tools or access resources exposed by the MCP server on behalf of the user in those limited circumstances. Note that running HTTP-based MCP servers locally without authentication is not recommended per MCP security best practices. This issue does not affect servers using stdio transport. This vulnerability is fixed in 1.24.0.	N/A	More Details
CVE-2025-66409	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In 5.5.1, 5.4.3, 5.3.4, 5.2.6, 5.1.6, and earlier, when AVRCP is enabled on ESP32, receiving a malformed VENDOR DEPENDENT command from a peer device can cause the Bluetooth stack to access memory before validating the command buffer length. This may lead to an out-of-bounds read, potentially exposing unintended memory content or causing unexpected behavior.	N/A	More Details
CVE-2025-65896	SQL injection vulnerability in long2ice assyncmy thru 0.2.10 allows attackers to execute arbitrary SQL commands via crafted dict keys.	N/A	More Details

CVE-2025-66201	LibreChat is a ChatGPT clone with additional features. Prior to version 0.8.1-rc2, LibreChat is vulnerable to Server-side Request Forgery (SSRF), by passing specially crafted OpenAPI specs to its "Actions" feature and making the LLM use those actions. It could be used by an authenticated user with access to this feature to access URLs only accessible to the LibreChat server (such as cloud metadata services, through which impersonation of the server might be possible). This issue has been patched in version 0.8.1-rc2.	N/A	More Details
CVE-2025-66221	Werkzeug is a comprehensive WSGI web application library. Prior to version 3.1.4, Werkzeug's safe_join function allows path segments with Windows device names. On Windows, there are special device names such as CON, AUX, etc that are implicitly present and readable in every directory. send_from_directory uses safe_join to safely serve files at user-specified paths under a directory. If the application is running on Windows, and the requested path ends with a special device name, the file will be opened successfully, but reading will hang indefinitely. This issue has been patched in version 3.1.4.	N/A	More Details
CVE-2025-66399	Cacti is an open source performance and fault management framework. Prior to 1.2.29, there is an input-validation flaw in the SNMP device configuration functionality. An authenticated Cacti user can supply crafted SNMP community strings containing control characters (including newlines) that are accepted, stored verbatim in the database, and later embedded into backend SNMP operations. In environments where downstream SNMP tooling or wrappers interpret newline-separated tokens as command boundaries, this can lead to unintended command execution with the privileges of the Cacti process. This vulnerability is fixed in 1.2.29.	N/A	More Details
CVE-2025-12848	Webform Multiple File Upload module for Drupal 7.x contains a cross-site scripting (XSS) vulnerability in the file name renderer. An unauthenticated attacker can exploit this vulnerability by uploading a file with a malicious filename containing JavaScript code (e.g., "<img src=1 onerror=alert(document.domain)>") to a Webform node with a Multifile field where file type validation is disabled. This allows the execution of arbitrary scripts in the context of the victim's browser. The issue is present in a third-party library and has been addressed in a patch available at https://github.com/fyneworks/multifile/pull/44 . Users are advised to apply the provided patch or update to a fixed version of the module.	N/A	More Details
CVE-2025-66265	CMService.exe creates the C:\\usr directory and subdirectories with insecure permissions, granting write access to all authenticated users. This allows attackers to replace configuration files (such as snmp.conf) or hijack DLLs to escalate privileges.	N/A	More Details
CVE-2025-66217	AIS-catcher is a multi-platform AIS receiver. Prior to version 0.64, an integer underflow vulnerability exists in the MQTT parsing logic of AIS-catcher. This vulnerability allows an attacker to trigger a massive Heap Buffer Overflow by sending a malformed MQTT packet with a manipulated Topic Length field. This leads to an immediate Denial of Service (DoS) and, when used as a library, severe Memory Corruption that can be leveraged for Remote Code Execution (RCE). This issue has been patched in version 0.64.	N/A	More Details
CVE-2025-66264	The CMService.exe service runs with SYSTEM privileges and contains an unquoted service path. This allows a local attacker with write privileges to the filesystem to insert a malicious executable in the path, leading to privilege escalation.	N/A	More Details
CVE-2025-66216	AIS-catcher is a multi-platform AIS receiver. Prior to version 0.64, a heap buffer overflow vulnerability has been identified in the AIS::Message class of AIS-catcher. This vulnerability allows an attacker to write approximately 1KB of arbitrary data into a 128-byte buffer. This issue has been patched in version 0.64.	N/A	More Details
CVE-2025-66219	willitmerge is a command line tool to check if pull requests are mergeable. In versions 0.2.1 and prior, there is a command Injection vulnerability in willitmerge. The vulnerability manifests in this package due to the use of insecure child process execution API (exec) to which it concatenates user input, whether provided to the command-line flag, or is in user control in the target repository. At time of publication, no known fix is public.	N/A	More Details
CVE-2025-66027	Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.6, an information disclosure vulnerability exposes participant details, including names and email addresses through the /api/trpc/polls.get,polls.participants.list endpoint, even when Pro privacy features are enabled. This bypasses intended privacy controls that should prevent participants from viewing other users' personal information. This issue has been patched in version 4.5.6.	N/A	More Details
	PostgreSQL SQL Injection (status_sql.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an		

CVE-2025-66260	attacker to perform SQL injection via sw1 and sw2 parameters in status_sql.php. The `status_sql.php` endpoint constructs SQL UPDATE queries by directly concatenating user-controlled `sw1` and `sw2` parameters without using parameterized queries or `pg_escape_string()`. While PostgreSQL's `pg_exec` limitations prevent stacked queries, attackers can inject subqueries for data exfiltration and leverage verbose error messages for reconnaissance.	N/A	More Details
CVE-2025-66263	Unauthenticated Arbitrary File Read via Null Byte Injection in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Null byte injection in download_setting.php allows reading arbitrary files. The `/var/tdf/download_setting.php` endpoint constructs file paths by concatenating user-controlled `$_GET['filename']` with a forced `.tgz` extension. Running on PHP 5.3.2 (pre-5.3.4), the application is vulnerable to null byte injection (%00), allowing attackers to bypass the extension restriction and traverse paths. By requesting `filename=../../../../etc/passwd%00`, the underlying C functions treat the null byte as a string terminator, ignoring the appended `.tgz` and enabling unauthenticated arbitrary file disclosure of any file readable by the web server user.	N/A	More Details
CVE-2025-13639	Inappropriate implementation in WebRTC in Google Chrome prior to 143.0.7499.41 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Low)	N/A	More Details
CVE-2025-12183	Out-of-bounds memory operations in org.lz4:lz4-java 1.8.0 and earlier allow remote attackers to cause denial of service and read adjacent memory via untrusted compressed input.	N/A	More Details
CVE-2025-66262	Arbitrary File Overwrite via Tar Extraction Path Traversal in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Tar extraction with -C / allow arbitrary file overwrite via crafted archive. The `restore_mozzi_memories.sh` script extracts user-controlled tar archives with `-C /` flag, depositing contents to the filesystem root without path validation. When combined with the unauthenticated file upload vulnerabilities (CVE-01, CVE-06, CVE-07), attackers can craft malicious .tgz archives containing path-traversed filenames (e.g., `etc/shadow`, `var/www/index.php`) to overwrite critical system files in writable directories, achieving full system compromise.	N/A	More Details
CVE-2025-66261	Unauthenticated OS Command Injection (restore_settings.php) in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform URL-decoded name parameter passed to exec() allows remote code execution. The `/var/tdf/restore_settings.php` endpoint passes user-controlled `$_GET["name"]` parameter through `urldecode()` directly into `exec()` without validation or escaping. Attackers can inject arbitrary shell commands using metacharacters (`;`, `|`, `&&`, etc.) to achieve unauthenticated remote code execution as the web server user.	N/A	More Details
CVE-2025-34352	JumpCloud Remote Assist for Windows versions prior to 0.317.0 include an uninstaller that is invoked by the JumpCloud Windows Agent as NT AUTHORITY\SYSTEM during agent uninstall or update operations. The Remote Assist uninstaller performs privileged create, write, execute, and delete actions on predictable files inside a user-writable %TEMP% subdirectory without validating that the directory is trusted or resetting its ACLs when it already exists. A local, low-privileged attacker can pre-create the directory with weak permissions and leverage mount-point or symbolic-link redirection to (a) coerce arbitrary file writes to protected locations, leading to denial of service (e.g., by overwriting sensitive system files), or (b) win a race to redirect DeleteFileW() to attacker-chosen targets, enabling arbitrary file or folder deletion and local privilege escalation to SYSTEM. This issue is fixed in JumpCloud Remote Assist 0.317.0 and affects Windows systems where Remote Assist is installed and managed through the Agent lifecycle.	N/A	More Details
CVE-2025-12638	Keras version 3.11.3 is affected by a path traversal vulnerability in the keras.utils.get_file() function when extracting tar archives. The vulnerability arises because the function uses Python's tarfile.extractall() method without the security-critical filter='data' parameter. Although Keras attempts to filter unsafe paths using filter_safe_paths(), this filtering occurs before extraction, and a PATH_MAX symlink resolution bug triggers during extraction. This bug causes symlink resolution to fail due to path length limits, resulting in a security bypass that allows files to be written outside the intended extraction directory. This can lead to arbitrary file writes outside the cache directory, enabling potential system compromise or malicious code execution.	N/A	More Details

	The vulnerability affects Keras installations that process tar archives with get_file() and does not affect versions where this extraction method is secured with the appropriate filter parameter.		
CVE-2025-60736	code-projects Online Medicine Guide 1.0 is vulnerable to SQL Injection in /login.php via the upass parameter.	N/A	More Details
CVE-2025-40700	Reflected Cross-Site Scripting (XSS) in IDI Eikon's Governalia. The vulnerability allows an attacker to execute JavaScript code in the victim's browser when a malicious URL with the 'q' parameter in '/search' is sent to them. This vulnerability can be exploited to steal sensitive information such as session cookies or to perform actions on behalf of the victim.	N/A	More Details
CVE-2025-66400	mdast-util-to-hast is an mdast utility to transform to hast. From 13.0.0 to before 13.2.1, multiple (unprefixed) classnames could be added in markdown source by using character references. This could make rendered user supplied markdown code elements appear like the rest of the page. This vulnerability is fixed in 13.2.1.	N/A	More Details
CVE-2025-12465	A Blind SQL injection vulnerability has been identified in QuickCMS. Improper neutralization of input provided by a high-privileged user into aFilesDelete allows for Blind SQL Injection attacks. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2020-36871	ESCAM QD-900 WIFI HD cameras contain an unauthenticated configuration disclosure vulnerability in the /web/cgi-bin/hi3510/backup.cgi endpoint. The endpoint allows remote download of a compressed configuration backup without requiring authentication or authorization. The exposed backup can include administrative credentials and other sensitive device settings, enabling an unauthenticated remote attacker to obtain information that may facilitate further compromise of the camera or connected network.	N/A	More Details
CVE-2025-65235	OpenCode Systems USSD Gateway OC Release: 5 Version 6.13.11 was discovered to contain a SQL injection vulnerability via the ID parameter in the getSubUsersByProvider function.	N/A	More Details
CVE-2025-65621	Snipe-IT before 8.3.4 allows stored XSS, allowing a low-privileged authenticated user to inject JavaScript that executes in an administrator's session, enabling privilege escalation.	N/A	More Details
CVE-2025-58044	JumpServer is an open source bastion host and an operation and maintenance security audit system. Prior to v3.10.19 and v4.10.5, The /core/i18n// endpoint uses the Referer header as the redirection target without proper validation, which could lead to an Open Redirect vulnerability. This vulnerability is fixed in v3.10.19 and v4.10.5.	N/A	More Details
CVE-2025-55749	XWiki is an open-source wiki software platform. From 16.7.0 to 16.10.11, 17.4.4, or 17.7.0, in an instance which is using the XWiki Jetty package (XJetty), a context is exposed to statically access any file located in the webapp/ folder. It allows accessing files which might contains credentials. Fixed in 16.10.11, 17.4.4, and 17.7.0.	N/A	More Details
CVE-2024-51999	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error and is not a valid vulnerability. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-65838	PublicCMS V5.202506.b is vulnerable to path traversal via the doUploadSitefile method.	N/A	More Details
CVE-2025-51683	A blind SQL Injection (SQLi) vulnerability in mJobtime v15.7.2 allows unauthenticated attackers to execute arbitrary SQL statements via a crafted POST request to the /Default.aspx/update_profile_Server endpoint .	N/A	More Details
CVE-2025-34297	KissFFT versions prior to the fix commit 1b083165 contain an integer overflow in kiss_fft_alloc() in kiss_fft.c on platforms where size_t is 32-bit. The nfft parameter is not validated before being used in a size calculation (sizeof(kiss_fft_cpx) * (nfft - 1)), which can wrap to a small value when nfft is large. As a result, malloc() allocates an undersized buffer and the subsequent twiddle-factor initialization loop writes nfft elements, causing a heap buffer overflow. This vulnerability only affects 32-bit architectures.	N/A	More Details

CVE-2025-13837	When loading a plist file, the plistlib module reads data in size specified by the file itself, meaning a malicious file can cause OOM and DoS issues	N/A	More Details
CVE-2025-13836	When reading an HTTP response from a server, if no read amount is specified, the default behavior will be to use Content-Length. This allows a malicious server to cause the client to read large amounts of data into memory, potentially causing OOM or other DoS.	N/A	More Details
CVE-2025-46175	Ruoyi v4.8.0 is vulnerable to Incorrect Access Control. There is a missing checkUserDataScope permission check in the authRole method of SysUserController.java.	N/A	More Details
CVE-2025-56396	An issue was discovered in Ruoyi 4.8.1 allowing attackers to gain escalated privileges due to the owning department having higher rights than the active user.	N/A	More Details
CVE-2025-50402	FAST FAC1200R F400_FAC1200R_Q is vulnerable to Buffer Overflow in the function sub_80435780 via the parameter string fac_password.	N/A	More Details
CVE-2019-25226	Dongyoung Media DM-AP240T/W wireless access points contain an unauthenticated configuration disclosure vulnerability in the /cgi-bin/sys_system_config management endpoint. The endpoint allows remote retrieval of a compressed configuration archive without requiring authentication or authorization. The exposed configuration may include administrative credentials and other sensitive settings, enabling an unauthenticated attacker to obtain information that can facilitate further compromise of the device or network.	N/A	More Details
CVE-2025-50399	FAST FAC1200R F400_FAC1200R_Q is vulnerable to Buffer Overflow in the function sub_80435780 via the parameter password.	N/A	More Details
CVE-2025-46174	Ruoyi v4.8.0 vulnerable to Incorrect Access Control. There is a missing checkUserDataScope permission check in the resetPwd Method of SysUserController.java.	N/A	More Details
CVE-2025-3747	Rejected reason: This CVE ID was duplicated of CVE-2025-32801	N/A	More Details
CVE-2025-65794	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-65793	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-65237	A reflected cross-site scripted (XSS) vulnerability in OpenCode Systems USSD Gateway OC Release: 5 allows attackers to execute arbitrary JavaScript in the context of a user's browser via injecting a crafted payload.	N/A	More Details
CVE-2025-66028	OneUptime is a solution for monitoring and managing online services. Prior to version 8.0.5567, OneUptime is vulnerable to privilege escalation via Login Response Manipulation. During the login process, the server response included a parameter called isMasterAdmin. By intercepting and modifying this parameter value from false to true, it is possible to gain access to the admin dashboard interface. However, an attacker may be unable to view or interact with the data if they still do not have sufficient permissions. This issue has been patched in version 8.0.5567.	N/A	More Details
CVE-2025-65966	OneUptime is a solution for monitoring and managing online services. In version 9.0.5598, a low-permission user can create new accounts through a direct API request instead of being restricted to the intended interface. This issue has been patched in version 9.1.0.	N/A	More Details
CVE-2025-	This admin plugin for Grav is an HTML user interface that provides a convenient way to configure Grav and easily create and modify pages. Prior to 1.11.0-beta.1, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the /admin/pages/[page] endpoint of the Grav application. This vulnerability allows attackers to inject malicious scripts into the data[header][template]	N/A	More Details

66310	parameter. The script is saved within the page's frontmatter and executed automatically whenever the affected content is rendered in the administrative interface or frontend view. This vulnerability is fixed in 1.11.0-beta.1.		
CVE-2025-66405	Portkey.ai Gateway is a blazing fast AI Gateway with integrated guardrails. Prior to 1.14.0, the gateway determined the destination baseURL by prioritizing the value in the x-portkey-custom-host request header. The proxy route then appends the client-specified path to perform an external fetch. This can be maliciously used by users for SSRF attacks. This vulnerability is fixed in 1.14.0.	N/A	More Details
CVE-2025-66410	Gin-vue-admin is a backstage management system based on vue and gin. In 2.8.6 and earlier, attackers can delete any file on the server at will, causing damage or unavailability of server resources. Attackers can control the 'FileMd5' parameter to delete any file and folder.	N/A	More Details
CVE-2025-66412	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 21.0.2, 20.3.15, and 19.2.17, A Stored Cross-Site Scripting (XSS) vulnerability has been identified in the Angular Template Compiler. It occurs because the compiler's internal security schema is incomplete, allowing attackers to bypass Angular's built-in security sanitization. Specifically, the schema fails to classify certain URL-holding attributes (e.g., those that could contain javascript: URLs) as requiring strict URL security, enabling the injection of malicious scripts. This vulnerability is fixed in 21.0.2, 20.3.15, and 19.2.17.	N/A	More Details
CVE-2025-66415	fastify-reply-from is a Fastify plugin to forward the current HTTP request to another server. Prior to 12.5.0, by crafting a malicious URL, an attacker could access routes that are not allowed, even though the reply.from is defined for specific routes in @fastify/reply-from. This vulnerability is fixed in 12.5.0.	N/A	More Details
CVE-2025-11461	Multiple SQL Injections in Frappe CRM Dashboard Controller due to unsafe concatenation of user-controlled parameters into dynamic SQL statements. This issue affects Frappe CRM: 1.53.1.	N/A	More Details
CVE-2025-66312	This admin plugin for Grav is an HTML user interface that provides a convenient way to configure Grav and easily create and modify pages. Prior to 1.11.0-beta.1, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the /admin/accounts/groups/Grupo endpoint of the Grav application. This vulnerability allows attackers to inject malicious scripts into the data[readableName] parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. This vulnerability is fixed in 1.11.0-beta.1.	N/A	More Details
CVE-2025-66311	This admin plugin for Grav is an HTML user interface that provides a convenient way to configure Grav and easily create and modify pages. Prior to 1.11.0-beta.1, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the /admin/pages/[page] endpoint of the Grav application. This vulnerability allows attackers to inject malicious scripts into the data[header][metadata], data[header][taxonomy][category], and data[header][taxonomy][tag] parameters. These scripts are stored in the page frontmatter and executed automatically whenever the affected page is accessed or rendered in the administrative interface. This vulnerability is fixed in 1.11.0-beta.1.	N/A	More Details
CVE-2025-55129	HackerOne community member Kassem S.(kassem_s94) has reported that username handling in Revive Adserver was still vulnerable to impersonation attacks after the fix for CVE-2025-52672, via several alternate techniques. Homoglyphs based impersonation has been independently reported by other HackerOne users, such as itz_hari_ and khoof.	N/A	More Details
CVE-2025-66309	This admin plugin for Grav is an HTML user interface that provides a convenient way to configure Grav and easily create and modify pages. Prior to 1.11.0-beta.1, a Reflected Cross-Site Scripting (XSS) vulnerability was identified in the /admin/pages/[page] endpoint of the Grav application. This vulnerability allows attackers to inject malicious scripts into the data[header][content][items] parameter. This vulnerability is fixed in 1.11.0-beta.1.	N/A	More Details
CVE-2025-66294	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, a Server-Side Template Injection (SSTI) vulnerability exists in Grav that allows authenticated attackers with editor permissions to execute arbitrary commands on the server and, under certain conditions, may also be exploited by unauthenticated attackers. This vulnerability stems from weak regex validation in the cleanDangerousTwig method. This vulnerability is fixed in 1.8.0-beta.27.	N/A	More Details
	This admin plugin for Grav is an HTML user interface that provides a convenient way to configure		

CVE-2025-66308	Grav and easily create and modify pages. Prior to 1.11.0-beta.1, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the /admin/config/site endpoint of the Grav application. This vulnerability allows attackers to inject malicious scripts into the data[taxonomies] parameter. The injected payload is stored on the server and automatically executed in the browser of any user who accesses the affected site configuration, resulting in a persistent attack vector. This vulnerability is fixed in 1.11.0-beta.1.	N/A	More Details
CVE-2025-66305	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, a Denial of Service (DoS) vulnerability was identified in the "Languages" submenu of the Grav admin configuration panel (/admin/config/system). Specifically, the Supported parameter fails to properly validate user input. If a malformed value is inserted—such as a single forward slash (/) or an XSS test string—it causes a fatal regular expression parsing error on the server. This leads to application-wide failure due to the use of the preg_match() function with an improperly constructed regular expression, resulting in an error. Once triggered, the site becomes completely unavailable to all users. This vulnerability is fixed in 1.8.0-beta.27.	N/A	More Details
CVE-2025-2486	The Ubuntu edk2 UEFI firmware packages accidentally allowed the UEFI Shell to be accessed in Secure Boot environments, possibly allowing bypass of Secure Boot constraints. Versions 2024.05-2ubuntu0.3 and 2024.02-2ubuntu0.3 disable the Shell. Some previous versions inserted a secure-boot-based decision to continue running inside the Shell itself, which is believed to be sufficient to enforce Secure Boot restrictions. This is an additional repair on top of the incomplete fix for CVE-2023-48733.	N/A	More Details
CVE-2025-66301	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, due to improper authorization checks when modifying critical fields on a POST request to /admin/pages/{page_name}, an editor with only permissions to change basic content on the form is now able to change the functioning of the form through modifying the content of the data[_json][header][form] which is the YAML frontmatter which includes the process section which dictates what happens after a user submits the form which include some important actions that could lead to further vulnerabilities. This vulnerability is fixed in 1.8.0-beta.27.	N/A	More Details
CVE-2025-65238	Incorrect access control in the getSubUsersByProvider function of OpenCode Systems USSD Gateway OC Release: 5 Version 6.13.11 allows attackers with low-level privileges to dump user records and access sensitive information.	N/A	More Details
CVE-2025-66298	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, having a simple form on site can reveal the whole Grav configuration details (including plugin configuration details) by using the correct POST payload to exploit a Server-Side Template (SST) vulnerability. Sensitive information may be contained in the configuration details. This vulnerability is fixed in 1.8.0-beta.27.	N/A	More Details
CVE-2025-65622	Snipe-IT before 8.3.4 allows stored XSS via the Locations "Country" field, enabling a low-privileged authenticated user to inject JavaScript that executes in another user's session.	N/A	More Details
CVE-2025-66297	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, a user with admin panel access and permissions to create or edit pages in Grav CMS can enable Twig processing in the page frontmatter. By injecting malicious Twig expressions, the user can escalate their privileges to admin or execute arbitrary system commands via the scheduler API. This results in both Privilege Escalation (PE) and Remote Code Execution (RCE) vulnerabilities. This vulnerability is fixed in 1.8.0-beta.27.	N/A	More Details
CVE-2019-25227	Tellion HN-2204AP routers contain an unauthenticated configuration disclosure vulnerability in the /cgi-bin/system_config_file management endpoint. The endpoint allows remote retrieval of a compressed configuration archive without requiring authentication or authorization. The exposed configuration may include administrative credentials, wireless keys, and other sensitive settings, enabling an unauthenticated attacker to obtain information that can facilitate further compromise of the device or network.	N/A	More Details
CVE-2020-36872	BACnet Test Server versions up to and including 1.01 contains a remote denial of service vulnerability in its BACnet/IP BVLC packet handling. The server fails to properly validate the BVLC Length field in incoming UDP BVLC frames on the default BACnet port (47808/udp). A remote unauthenticated attacker can send a malformed BVLC Length value to trigger an access violation and crash the application, resulting in a denial of service.	N/A	More Details
	ChurchCRM is an open-source church management system. In ChurchCRM 6.2.0 and earlier,		

CVE-2025-66313	there is a time-based blind SQL injection in the handling of the 1FieldSec parameter. Injecting SLEEP() causes deterministic server-side delays, proving the value is incorporated into a SQL query without proper parameterization. The issue allows data exfiltration and modification via blind techniques.	N/A	More Details
CVE-2020-36873	Astak CM-818T3 2.4GHz wireless security surveillance cameras contain an unauthenticated configuration disclosure vulnerability in the /web/cgi-bin/hi3510/backup.cgi endpoint. The endpoint permits remote download of a compressed configuration backup without requiring authentication or authorization. The exposed backup may include administrative credentials and other sensitive device settings, enabling an unauthenticated remote attacker to obtain information that could facilitate further compromise of the camera or connected network.	N/A	More Details
CVE-2025-66228	Rejected reason: Not used	N/A	More Details
CVE-2025-34351	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. At the request of the MITRE TL-Root and following the CVE Program’s Dispute Policy, it has been determined that this assignment did not identify a valid vulnerability based on the vendor's product security model.	N/A	More Details
CVE-2025-13871	Cross-Site Request Forgery (CSRF) in the resource-management feature of ObjectPlanet Opinio 7.26 rev12562 allows to upload files on behalf of the connected users and then access such files without authentication.	N/A	More Details
CVE-2025-13872	Blind Server-Side Request Forgery (SSRF) in the survey-import feature of ObjectPlanet Opinio 7.26 rev12562 on Web-based platforms allows an attacker to force the server to perform HTTP GET requests via crafted import requests to an arbitrary destination.	N/A	More Details
CVE-2025-13873	Stored Cross-Site Scripting (XSS) in the survey-import feature of ObjectPlanet Opinio 7.26 rev12562 on web application allows an attacker to inject arbitrary JavaScript code, which executes in the browsing context of any visitor accessing the compromised survey.	N/A	More Details
CVE-2025-13353	In gokey versions <0.2.0, a flaw in the seed decryption logic resulted in passwords incorrectly being derived solely from the initial vector and the AES-GCM authentication tag of the key seed. This issue has been fixed in gokey version 0.2.0. This is a breaking change. The fix has invalidated any passwords/secrets that were derived from the seed file (using the -s option). Even if the input seed file stays the same, version 0.2.0 gokey will generate different secrets. Impact This vulnerability impacts generated keys/secrets using a seed file as an entropy input (using the -s option). Keys/secrets generated just from the master password (without the -s option) are not impacted. The confidentiality of the seed itself is also not impacted (it is not required to regenerate the seed itself). Specific impact includes: * keys/secrets generated from a seed file may have lower entropy: it was expected that the whole seed would be used to generate keys (240 bytes of entropy input), where in vulnerable versions only 28 bytes was used * a malicious entity could have recovered all passwords, generated from a particular seed, having only the seed file in possession without the knowledge of the seed master password Patches The code logic bug has been fixed in gokey version 0.2.0 and above. Due to the deterministic nature of gokey, fixed versions will produce different passwords/secrets using seed files, as all seed entropy will be used now. System secret rotation guidance It is advised for users to regenerate passwords/secrets using the patched version of gokey (0.2.0 and above), and provision/rotate these secrets into respective systems in place of the old secret. A specific rotation procedure is system-dependent, but most common patterns are described below. Systems that do not require the old password/secret for rotation Such systems usually have a "Forgot password" facility or a similar facility allowing users to rotate their password/secrets by sending a unique "magic" link to the user's email or phone. In such cases users are advised to use this facility and input the newly generated password secret, when prompted by the system. Systems that require the old password/secret for rotation Such systems usually have a modal password rotation window usually in the user settings section requiring the user to input the old and the new password sometimes with a confirmation. To generate/recover the old password in such cases users are advised to: * temporarily download gokey version 0.1.3 https://github.com/cloudflare/gokey/releases/tag/v0.1.3 for their respective operating system to recover the old password * use gokey version 0.2.0 or above to generate the new password * populate the system provided password rotation form Systems that allow multiple credentials for the same account to be provisioned Such systems usually require a secret or a cryptographic key as a credential for access, but allow several credentials at the same time. One example is	N/A	More Details

	SSH: a particular user may have several authorized public keys configured on the SSH server for access. For such systems users are advised to: * generate a new secret/key/credential using gokey version 0.2.0 or above * provision the new secret/key/credential in addition to the existing credential on the system * verify that the access or required system operation is still possible with the new secret/key/credential * revoke authorization for the existing/old credential from the system Credit This vulnerability was found by Théo Cusnir (@mister_mime https://hackerone.com/mister_mime) and responsibly disclosed through Cloudflare's bug bounty program.		
CVE-2025-49643	An authenticated Zabbix user (including Guest) is able to cause disproportionate CPU load on the webserver by sending specially crafted parameters to /imgstore.php, leading to potential denial of service.	N/A	More Details
CVE-2025-49642	Library loading on AIX Zabbix Agent builds can be hijacked by local users with write access to the /home/cecuser directory.	N/A	More Details
CVE-2025-11778	Stack-based buffer overflow in Circutor SGE-PLC1000/SGE-PLC50 v0.9.2. This vulnerability allows an attacker to remotely exploit memory corruption through the 'read_packet()' function of the TACACSPLUS implementation.	N/A	More Details
CVE-2025-11779	Stack-based buffer overflow vulnerability in CircutorSGE-PLC1000/SGE-PLC50 v9.0.2. The 'SetLan' function is invoked when a new configuration is applied. This new configuration function is activated by a management web request, which can be invoked by a user when making changes to the 'index.cgi' web application. The parameters are not being sanitised, which could lead to command injection.	N/A	More Details
CVE-2025-11780	Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'showMeterReport()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for the “meter” parameter.	N/A	More Details
CVE-2025-11781	Use of hardcoded cryptographic keys in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The affected firmware contains a hardcoded static authentication key. An attacker with local access to the device can extract this key (e.g., by analysing the firmware image or memory dump) and create valid firmware update packages. This bypasses all intended access controls and grants full administrative privileges.	N/A	More Details
CVE-2025-11782	Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The 'ShowDownload()' function uses “sprintf()” to format a string that includes the user-controlled input of 'GetParameter(meter)' in the fixed-size buffer 'acStack_4c' (64 bytes) without checking the length. An attacker can provide an excessively long value for the 'meter' parameter that exceeds the 64-byte buffer size.	N/A	More Details
CVE-2025-11783	Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The vulnerability is found in the 'AddEvent()' function when copying the user-controlled username input to a fixed-size buffer (48 bytes) without boundary checking. This can lead to memory corruption, resulting in possible remote code execution.	N/A	More Details
CVE-2025-11784	Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowMeterDatabase()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for the 'meter' parameter.	N/A	More Details
CVE-2025-11785	Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowMeterPasswords()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for the 'meter' parameter.	N/A	More Details
CVE-2025-11786	Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'SetUserPassword()' function, the 'newPassword' parameter is directly embedded in a shell command string using 'sprintf()' without any sanitisation or validation, and then executed using 'system()'. This allows an attacker to inject arbitrary shell commands that will be executed with	N/A	More Details

	the same privileges as the application.		
CVE-2025-11787	Command injection vulnerability in the operating system in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2 through the 'GetDNS()', 'CheckPing()' and 'TraceRoute()' functions.	N/A	More Details
CVE-2025-11788	Heap-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowSupervisorParameters()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the user input, which is directly incorporated into a buffer without size validation. An attacker can provide an excessively large input for the 'meter' parameter.	N/A	More Details
CVE-2025-13762	Improper Input Validation vulnerability in CyberArk CyberArk Secure Web Sessions Extension on Chrome, Edge allows Denial of Service when trying to starting new SWS sessions.This issue affects CyberArk Secure Web Sessions Extension: before 2.2.30305.	N/A	More Details
CVE-2025-66229	Rejected reason: Not used	N/A	More Details
CVE-2025-10543	In Eclipse Paho Go MQTT v3.1 library (paho.mqtt.golang) versions <=1.5.0 UTF-8 encoded strings, passed into the library, may be incorrectly encoded if their length exceeds 65535 bytes. This may lead to unexpected content in packets sent to the server (for example, part of an MQTT topic may leak into the message body in a PUBLISH packet). The issue arises because the length of the data passed in was converted from an int64/int32 (depending upon CPU) to an int16 without checks for overflows. The int16 length was then written, followed by the data (e.g. topic). This meant that when the data (e.g. topic) was over 65535 bytes then the amount of data written exceeds what the length field indicates. This could lead to a corrupt packet, or mean that the excess data leaks into another field (e.g. topic leaks into message body).	N/A	More Details
CVE-2025-66233	Rejected reason: Not used	N/A	More Details
CVE-2025-64983	Smart Video Doorbell firmware versions prior to 2.01.078 contain an active debug code vulnerability that allows an attacker to connect via Telnet and gain access to the device.	N/A	More Details
CVE-2025-66235	Rejected reason: Not used	N/A	More Details
CVE-2025-66234	Rejected reason: Not used	N/A	More Details
CVE-2020-36874	ACE SECURITY WIP-90113 HD cameras contain an unauthenticated configuration disclosure vulnerability in the /web/cgi-bin/hi3510/backup.cgi endpoint. The endpoint permits remote download of a compressed configuration backup without requiring authentication or authorization. The exposed backup may include administrative credentials and other sensitive device settings, enabling an unauthenticated remote attacker to obtain information that could facilitate further compromise of the camera or connected network.	N/A	More Details
CVE-2025-62593	Ray is an AI compute engine. Prior to version 2.52.0, developers working with Ray as a development tool can be exploited via a critical RCE vulnerability exploitable via Firefox and Safari. This vulnerability is due to an insufficient guard against browser-based attacks, as the current defense uses the User-Agent header starting with the string "Mozilla" as a defense mechanism. This defense is insufficient as the fetch specification allows the User-Agent header to be modified. Combined with a DNS rebinding attack against the browser, and this vulnerability is exploitable against a developer running Ray who inadvertently visits a malicious website, or is served a malicious advertisement (malvertising). This issue has been patched in version 2.52.0.	N/A	More Details
CVE-2025-66030	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. An Integer Overflow vulnerability in node-forge versions 1.3.1 and below enables remote, unauthenticated attackers to craft ASN.1 structures containing OIDs with oversized arcs. These arcs may be decoded as smaller, trusted OIDs due to 32-bit bitwise truncation, enabling the bypass of downstream OID-based security decisions. This issue has been patched in version	N/A	More Details

	1.3.2.		
CVE-2025-66031	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. An Uncontrolled Recursion vulnerability in node-forge versions 1.3.1 and below enables remote, unauthenticated attackers to craft deep ASN.1 structures that trigger unbounded recursive parsing. This leads to a Denial-of-Service (DoS) via stack exhaustion when parsing untrusted DER inputs. This issue has been patched in version 1.3.2.	N/A	More Details
CVE-2025-66035	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to versions 19.2.16, 20.3.14, and 21.0.1, there is a XSRF token leakage via protocol-relative URLs in angular HTTP clients. The vulnerability is a Credential Leak by App Logic that leads to the unauthorized disclosure of the Cross-Site Request Forgery (XSRF) token to an attacker-controlled domain. Angular's HttpClient has a built-in XSRF protection mechanism that works by checking if a request URL starts with a protocol (http:// or https://) to determine if it is cross-origin. If the URL starts with protocol-relative URL (//), it is incorrectly treated as a same-origin request, and the XSRF token is automatically added to the X-XSRF-TOKEN header. This issue has been patched in versions 19.2.16, 20.3.14, and 21.0.1. A workaround for this issue involves avoiding using protocol-relative URLs (URLs starting with //) in HttpClient requests. All backend communication URLs should be hardcoded as relative paths (starting with a single /) or fully qualified, trusted absolute URLs.	N/A	More Details
CVE-2025-66232	Rejected reason: Not used	N/A	More Details
CVE-2025-13829	Incorrect Authorization vulnerability in Data Illusion Zumbrunn NGSurvey allows any logged-in user to obtain the private information of any other user. Critical information retrieved: * APIKEY (1 year user Session) * RefreshToken (10 minutes user Session) * Password hashed with bcrypt * User IP * Email * Full Name	N/A	More Details
CVE-2025-66231	Rejected reason: Not used	N/A	More Details
CVE-2025-61229	An issue in Shirt Pocket's SuperDuper! 3.10 and earlier allow a local attacker to modify the default task template to execute an arbitrary preflight script with root privileges and Full Disk Access, thus bypassing macOS privacy controls.	N/A	More Details
CVE-2025-66230	Rejected reason: Not used	N/A	More Details
CVE-2024-5539	The Access Control Bypass vulnerability found in ALC WebCTRL and Carrier i-Vu in versions up to and including 8.5 allows a malicious actor to bypass intended access restrictions and expose sensitive information via the web based building automation server.	N/A	More Details
CVE-2024-5540	The reflective cross-site scripting vulnerability found in ALC WebCTRL and Carrier i-Vu in versions older than 8.0 affects login panels allowing a malicious actor to compromise the client browser .	N/A	More Details
CVE-2025-0657	A weakness in Automated Logic and Carrier i-Vu Gen5 router on driver version drv_gen5_106-01-2380, allows malformed packets to be sent through BACnet MS/TP network causing the devices to enter a fault state. This fault state requires a manual power cycle to return the device to network visibility.	N/A	More Details
CVE-2025-10971	Insecure Storage of Sensitive Information vulnerability in MeetMe on iOS, Android allows Retrieve Embedded Sensitive Data. This issue affects MeetMe: through v2.2.5.	N/A	More Details
CVE-2025-0658	A vulnerability in Automated Logic and Carrier's Zone Controller via BACnet protocol causes the device to crash. The device enters a fault state; after a reset, a second packet can leave it permanently unresponsive until a manual power cycle is performed.	N/A	More Details
CVE-2025-	Out-of-bounds read vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The 'DownloadFile' function converts a parameter to an integer using 'atoi()' and then uses it as an index in the 'FilesDownload' array with '(&FilesDownload)[iVar2]'. If the parameter is too large, it will access	N/A	More Details

11789	memory beyond the limits.		