SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 November 2025

Generated on 19 November 2025

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-36250	IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 NIM server (formerly known as NIM master) service (nimesis) could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously addressed in CVE-2024-56346.	10.0	More Details
CVE-2025-58083	General Industrial Controls Lynx+ Gateway is missing critical authentication in the embedded web server which could allow an attacker to remotely reset the device.	10.0	More Details
CVE-2025-54339	An Incorrect Access Control vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 exploitable remotely for Escalation of Privileges.	10.0	More Details
CVE-2025-12870	The a+HRD developed by aEnrich has an Authentication Abuse vulnerability, allowing unauthenticated remote attackers to send crafted packets to obtain administrator access tokens and use them to access the system with elevated privileges.	9.8	More Details
CVE-2025-41734	An unauthenticated remote attacker can execute arbitrary php files and gain full access of the affected devices.	9.8	More Details
CVE-2025-41733	The commissioning wizard on the affected devices does not validate if the device is already initialized. An unauthenticated remote attacker can construct POST requests to set root credentials.	9.8	More Details
CVE-2024-44659	PHPGurukul Online Shopping Portal 2.0 is vulnerable to SQL Injection via the email parameter in forgot-password.php.	9.8	More Details
CVE-2025-63747	QaTraq 6.9.2 ships with administrative account credentials which are enabled in default installations and permit immediate login via the web application login page. Because the account provides administrative privileges in the default configuration, an attacker who can reach the login page can gain administrative access.	9.8	More Details
CVE-2025-13284	ThinPLUS developed by ThinPLUS has an OS Command Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the server.	9.8	More Details
CVE-2025-13188	A vulnerability was detected in D-Link DIR-816L 2_06_b09_beta. Affected by this vulnerability is the function authenticationcgi_main of the file /authentication.cgi. Performing manipulation of the argument Password results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details

CVE-2025-64446	A relative path traversal vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.4, FortiWeb 7.4.0 through 7.4.9, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow an attacker to execute administrative commands on the system via crafted HTTP or HTTPS requests.	9.8	More Details
CVE-2025-12871	The a+HRD developed by aEnrich has an Authentication Abuse vulnerability, allowing unauthenticated remote attackers to craft administrator access tokens and use them to access the system with elevated privileges.	9.8	More Details
CVE-2025-9312	A missing authentication enforcement vulnerability exists in the mutual TLS (mTLS) implementation used by System REST APIs and SOAP services in multiple WSO2 products. Due to improper validation of client certificate–based authentication in certain default configurations, the affected components may permit unauthenticated requests even when mTLS is enabled. This condition occurs when relying on the default mTLS settings for System REST APIs or when the mTLS authenticator is enabled for SOAP services, causing these interfaces to accept requests without enforcing additional authentication. Successful exploitation allows a malicious actor with network access to the affected endpoints to gain administrative privileges and perform unauthorized operations. The vulnerability is exploitable only when the impacted mTLS flows are enabled and accessible in a given deployment. Other certificate-based authentication mechanisms such as Mutual TLS OAuth client authentication and X.509 login flows are not affected, and APIs served through the API Gateway of WSO2 API Manager remain unaffected.	9.8	More Details
CVE-2025-63353	A vulnerability in FiberHome GPON ONU HG6145F1 RP4423 allows the device's factory default Wi-Fi password (WPA/WPA2 pre-shared key) to be predicted from the SSID. The device generates default passwords using a deterministic algorithm that derives the router passphrase from the SSID, enabling an attacker who can observe the SSID to predict the default password without authentication or user interaction.	9.8	More Details
CVE-2025-64280	A SQL Injection Vulnerability in CentralSquare Community Development 19.5.7 allows attackers to inject SQL via the permit_no field.	9.8	More Details
CVE-2025-63666	Tenda AC15 v15.03.05.18_multi) issues an authentication cookie that exposes the account password hash to the client and uses a short, low-entropy suffix as the session identifier. An attacker with network access or the ability to run JS in a victim browser can steal the cookie and replay it to access protected resources.	9.8	More Details
CVE-2025-11366	N-central < 2025.4 is vulnerable to authentication bypass via path traversal	9.8	More Details
CVE-2025-63679	free5gc v4.1.0 and before is vulnerable to Buffer Overflow. When AMF receives an UplinkRANConfigurationTransfer NGAP message from a gNB, the AMF process crashes.	9.8	More Details
CVE-2025-56385	A SQL injection vulnerability exists in the login functionality of WellSky Harmony version 4.1.0.2.83 within the 'xmHarmony.asp' endpoint. User-supplied input to the 'TXTUSERID' parameter is not properly sanitized before being incorporated into a SQL query. Successful authentication may lead to authentication bypass, data leakage, or full system compromise of backend database contents.	9.8	More Details
CVE-2025-11367	The N-central Software Probe < 2025.4 is vulnerable to Remote Code Execution via deserialization	9.8	More Details
CVE-2025-64281	An Authentication Bypass issue in CentralSquare Community Development 19.5.7 allows attackers to access the admin panel without admin credentials.	9.8	More Details
CVE-2025-64709	Typebot is an open-source chatbot builder. In versions prior to 3.13.1, a Server-Side Request Forgery (SSRF) vulnerability in the Typebot webhook block (HTTP Request component) functionality allows authenticated users to make arbitrary HTTP requests from the server, including access to AWS Instance Metadata Service (IMDS). By bypassing IMDSv2 protection through custom header injection, attackers can extract temporary AWS IAM credentials for the EKS node role, leading to complete compromise of the Kubernetes cluster and associated AWS infrastructure. Version 3.13.1 fixes the issue.	9.6	More Details
CVE-2025-54343	An Incorrect Access Control vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 exploitable remotely for Escalation of Privileges.	9.6	More Details
CVE-2025-36251	IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 nimsh service SSL/TLS implementations could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously addressed in CVE-2024-56347.	9.6	More Details
CVE-2025-63289	Sogexia Android App Compile Affected SDK v35, Max SDK 32 and fixed in v36, was discovered to contain hardcoded encryption keys in the encryption_helper.dart file	9.1	More Details
CVE-2025-40547	A logic error vulnerability exists in Serv-U which when abused could give a malicious actor with access to admin privileges the ability to execute code. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.	9.1	More Details

CVE-2025-40548	A missing validation process exists in Serv U when abused, could give a malicious actor with access to admin privileges the ability to execute code. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium because services frequently run under less-privileged service accounts by default.	9.1	More Details
CVE-2025-40549	A Path Restriction Bypass vulnerability exists in Serv-U that when abused, could give a malicious actor with access to admin privileges the ability to execute code on a directory. This issue requires administrative privileges to abuse. On Windows systems, this scored as medium due to differences in how paths and home directories are handled.	9.1	More Details
CVE-2025-46608	Dell Data Lakehouse, versions prior to 1.6.0.0, contain(s) an Improper Access Control vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges. This vulnerability is considered Critical, as it may result in unauthorized access with elevated privileges, compromising system integrity and customer data. Dell recommends customers upgrade to the latest version at the earliest opportunity.	9.1	More Details
CVE-2025-12762	pgAdmin versions up to 9.9 are affected by a Remote Code Execution (RCE) vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. This issue allows attackers to inject and execute arbitrary commands on the server hosting pgAdmin, posing a critical risk to the integrity and security of the database management system and underlying data.	9.1	More Details
CVE-2025-36096	IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 stores NIM private keys used in NIM environments in an insecure way which is susceptible to unauthorized access by an attacker using man in the middle techniques.	9.0	More Details
CVE-2025-9501	The W3 Total Cache WordPress plugin before 2.8.13 is vulnerable to command injection via the _parse_dynamic_mfunc function, allowing unauthenticated users to execute PHP commands by submitting a comment with a malicious payload to a post.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-13088	The Category and Product Woocommerce Tabs plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.0. This is due to insufficient input validation on the 'template' parameter in the categoryProductTab() function. This makes it possible for authenticated attackers, with contributor level access and above, to include and execute arbitrary .php files on the server.	8.8	More Details
CVE-2025-41736	A low privileged remote attacker can upload a new or overwrite an existing python script by using a path traversal of the target filename in php resulting in a remote code execution.	8.8	More Details
CVE-2025-57310	A Cross-Site Request Forgery (CSRF) vulnerability in Salmen2/Simple-Faucet-Script v1.07 via crafted POST request to admin.php?p=ads&c=1 allowing attackers to execute arbitrary code.	8.8	More Details
CVE-2025-13042	Inappropriate implementation in V8 in Google Chrome prior to 142.0.7444.166 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-2843	A flaw was found in the Observability Operator. The Operator creates a ServiceAccount with *ClusterRole* upon deployment of the *Namespace-Scoped* Custom Resource MonitorStack. This issue allows an adversarial Kubernetes Account with only namespaced-level roles, for example, a tenant controlling a namespace, to create a MonitorStack in the authorized namespace and then elevate permission to the cluster level by impersonating the ServiceAccount created by the Operator, resulting in privilege escalation and other issues.	8.8	More Details
CVE-2025-13258	A vulnerability was detected in Tenda AC20 up to 16.03.08.12. The impacted element is an unknown function of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto results in buffer overflow. The attack can be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-12733	The Import any XML, CSV or Excel File to WordPress (WP All Import) plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.9.6. This is due to the use of eval() on unsanitized user-supplied input in the pmxi_if function within helpers/functions.php. This makes it possible for authenticated attackers, with import capabilities (typically administrators), to inject and execute arbitrary PHP code on the server via crafted import templates. This can lead to remote code execution.	8.8	More Details
	The LifterLMS – WP LMS for eLearning, Online Courses, & Quizzes plugin for WordPress is vulnerable to privilege escalation. This is due to the plugin not properly validating a user's identity prior to allowing them to		

CVE-2025-11923	modify their own role via the REST API. The permission check in the update_item_permissions_check() function returns true when a user updates their own account without verifying the role changes. This makes it possible for authenticated attackers, with student-level access and above, to escalate their privileges to administrator by updating their own roles array via a crafted REST API request. Another endpoint intended for instructors also provides an attack vector. Affected version ranges are 3.5.3-3.41.2, 4.0.0-4.21.3, 5.0.0-5.10.0, 6.0.0-6.11.0, 7.0.0-7.8.7, 8.0.0-8.0.7, 9.0.0-9.0.7, 9.1.0.	8.8	More Details
CVE-2025-58692	An improper neutralization of special elements used in an SQL Command ("SQL Injection") vulnerability [CWE-89] in Fortinet FortiVoice 7.2.0 through 7.2.2, FortiVoice 7.0.0 through 7.0.7 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP or HTTPS requests.	8.8	More Details
CVE-2025-6670	A Cross-Site Request Forgery (CSRF) vulnerability exists in multiple WSO2 products due to the use of the HTTP GET method for state-changing operations within admin services, specifically in the event processor of the Carbon console. Although the SameSite=Lax cookie attribute is used as a mitigation, it is ineffective in this context because it allows cookies to be sent with cross-origin top-level navigations using GET requests. A malicious actor can exploit this vulnerability by tricking an authenticated user into visiting a crafted link, leading the browser to issue unintended state-changing requests. Successful exploitation could result in unauthorized operations such as data modification, account changes, or other administrative actions. According to WSO2 Secure Production Guidelines, exposure of Carbon console services to untrusted networks is discouraged, which may reduce the impact in properly secured deployments.	8.8	More Details
CVE-2025-13288	A security vulnerability has been detected in Tenda CH22 1.0.0.1. This impacts the function fromPptpUserSetting of the file /goform/PPTPUserSetting. The manipulation of the argument delno leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-63748	QaTraq 6.9.2 allows authenticated users to upload arbitrary files via the "Add Attachment" feature in the "Test Script" module. The application fails to restrict file types, enabling the upload of executable PHP files. Once uploaded, the file can be accessed through the "View Attachment" option, which executes the PHP payload on the server.	8.8	More Details
CVE-2025-13319	An injection vulnerability has been discovered in the API feature in Digi On-Prem Manager, enabling an attacker with valid API tokens to inject SQL via crafted input. The API is not enabled by default, and a valid API token is required to perform the attack.	8.8	More Details
CVE-2025-12775	The WP Dropzone plugin for WordPress is vulnerable to authenticated arbitrary file upload in all versions up to, and including, 1.1.0 via the `ajax_upload_handle` function. This is due to the chunked upload functionality writing files directly to the uploads directory before any file type validation occurs. This makes it possible for authenticated attackers, with subscriber 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
CVE-2025-13223	Type Confusion in V8 in Google Chrome prior to 142.0.7444.175 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-13224	Type Confusion in V8 in Google Chrome prior to 142.0.7444.175 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-13227	Type Confusion in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-13304	A security flaw has been discovered in D-Link DWR-M920, DWR-M921, DWR-M960, DWR-M961 and DIR-825M 1.01.07/1.1.47. This vulnerability affects unknown code of the file /boafrm/formPingDiagnosticRun. Performing manipulation of the argument host results in buffer overflow. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	8.8	More Details
CVE-2025-46428	Dell SmartFabric OS10 Software, versions prior to 10.6.1.0, contain an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Code execution.	8.8	More Details
CVE-2025-13226	Type Confusion in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-36553	A buffer overflow vulnerability exists in the CvManager functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted ControlVault API call can lead to memory corruption. An attacker can issue an api call to trigger this vulnerability.	8.8	More Details
CVE-2025-46427	Dell SmartFabric OS10 Software, versions prior to 10.6.1.0, contain an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	8.8	More Details

CVE-2025-13305	A weakness has been identified in D-Link DWR-M920, DWR-M921, DWR-M960, DIR-822K and DIR-825M 1.01.07. This issue affects some unknown processing of the file /boafrm/formTracerouteDiagnosticRun. Executing manipulation of the argument host can lead to buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-13191	A vulnerability was determined in D-Link DIR-816L 2_06_b09_beta. This issue affects the function soapcgi_main of the file /soap.cgi. This manipulation causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-20341	A vulnerability in Cisco Catalyst Center Virtual Appliance could allow an authenticated, remote attacker to elevate privileges to Administrator on an affected system. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected system. A successful exploit could allow the attacker to perform unauthorized modifications to the system, including creating new user accounts or elevating their own privileges on an affected system. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Observer.	8.8	More Details
CVE-2025-13190	A vulnerability was found in D-Link DIR-816L 2_06_b09_beta. This vulnerability affects the function scandir_main of the file /portal/__ajax_exporer.sgi. The manipulation of the argument en results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-43515	The issue was addressed by refusing external connections by default. This issue is fixed in Compressor 4.11.1. An unauthenticated user on the same network as a Compressor server may be able to execute arbitrary code.	8.8	More Details
CVE-2025-8693	A post-authentication command injection vulnerability in the "priv" parameter of Zyxel DX3300-T0 firmware version 5.50(ABVY.6.3)C0 and earlier could allow an authenticated attacker to execute operating system (OS) commands on an affected device.	8.8	More Details
CVE-2025-13230	Type Confusion in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-60679	A stack buffer overflow vulnerability exists in the D-Link DIR-816A2 router firmware DIR-816A2_FWv1.10CNB05_R1B011D88210.img in the upload.cgi module, which handles firmware version information. The vulnerability occurs because /proc/version is read into a 512-byte buffer and then concatenated using sprintf() into another 512-byte buffer containing a 29-byte constant. Input exceeding 481 bytes triggers a stack buffer overflow, allowing an attacker who can control /proc/version content to potentially execute arbitrary code on the device.	8.8	More Details
CVE-2025-13229	Type Confusion in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-60690	A stack-based buffer overflow exists in the get_merge_ipaddr function of the httpd binary on Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz). The function concatenates up to four user-supplied CGI parameters matching <parameter>_0~3 into a fixed-size buffer (a2) without bounds checking. Remote attackers can exploit this vulnerability via specially crafted HTTP requests to execute arbitrary code or cause denial of service without authentication.	8.8	More Details
CVE-2025-13069	The Enable SVG, WebP, and ICO Upload plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 1.1.2. This is due to insufficient file type validation detecting ICO files, allowing double extension files with the appropriate magic bytes to bypass sanitization while being accepted as a valid ICO file. This makes it possible for authenticated attackers, with author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-13228	Type Confusion in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-63406	An issue in Intermesh BV GroupOffice vulnerable before v.25.0.47 and 6.8.136 allows a remote attacker to execute arbitrary code via the dbToApi() and eval() in the FunctionField.php	8.8	More Details
CVE-2025-32089	A buffer overflow vulnerability exists in the CvManager_SBI functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted ControlVault API call can lead to a arbitrary code execution. An attacker can issue an api call to trigger this vulnerability.	8.8	More Details
CVE-2025-	A vulnerability has been found in D-Link DIR-816L 2_06_b09_beta. This affects the function genacgi_main of the file gena.cgi. The manipulation of the argument SERVER_ID/HTTP_SID leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and	8.8	More Details

13189	may be used. This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2025-41735	A low privileged remote attacker can upload any file to an arbitrary location due to missing file check resulting in remote code execution.	8.8	More Details
CVE-2025-60691	A stack-based buffer overflow exists in the httpd binary of Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz). The apply_cgi and block_cgi functions copy user-supplied input from the "url" CGI parameter into stack buffers (v36, v29) using sprintf without bounds checking. Because these buffers are allocated as single-byte variables, any non-empty input will trigger a buffer overflow. Remote attackers can exploit this vulnerability via crafted HTTP requests to execute arbitrary code or cause denial of service without authentication.	8.8	More Details
CVE-2025-64186	Evervault is a payment security solution. A vulnerability was identified in the `evervault-go` SDK's attestation verification logic in versions of `evervault-go` prior to 1.3.2 that may allow incomplete documents to pass validation. This may cause the client to trust an enclave operator that does not meet expected integrity guarantees. The exploitability of this issue is limited in Evervault-hosted environments as an attacker would require the pre-requisite ability to serve requests from specific evervault domain names, following from our ACME challenge based TLS certificate acquisition pipeline. The vulnerability primarily affects applications which only check PCR8. Though the efficacy is also reduced for applications that check all PCR values, the impact is largely remediated by checking PCR 0, 1 and 2. The identified issue has been addressed in version 1.3.2 by validating attestation documents before storing in the cache, and replacing the naive equality checks with a new SatisfiedBy check. Those who useevervault-go to attest Enclaves that are hosted outside of Evervault environments and cannot upgrade have two possible workarounds available. Modify the application logic to fail verification if PCR8 is not explicitly present and non-empty and/or add custom pre-validation to reject documents that omit any required PCRs.	8.7	More Details
CVE-2025-31649	A hard-coded password vulnerability exists in the ControlVault WBDI Driver functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted ControlVault API call can lead to execute priviledged operation. An attacker can issue an api call to trigger this vulnerability.	8.7	More Details
CVE-2025-31361	A privilege escalation vulnerability exists in the ControlVault WBDI Driver WBIO_USH_ADD_RECORD functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted WinBioControlUnit call can lead to privilege escalation. An attacker can issue an api call to trigger this vulnerability.	8.7	More Details
CVE-2025-63680	Nero BackItUp in the Nero Productline is vulnerable to a path parsing/UI rendering flaw (CWE-22) that, in combination with Windows ShellExecuteW fallback extension resolution, leads to arbitrary code execution when a user clicks a crafted entry. By creating a trailing-dot folder and placing a same-basename script, Nero BackItUp renders the file as a folder icon and then invokes ShellExecuteW, which executes the script via PATHEXT fallback (.COM/.EXE/.BAT/.CMD). The issue affects recent Nero BackItUp product lines (2019-2025 and earlier) and has been acknowledged by the vendor.	8.6	More Details
CVE-2025-64309	Brightpick Mission Control discloses device telemetry, configuration, and credential information via WebSocket traffic to unauthenticated users when they connect to a specific URL. The unauthenticated URL can be discovered through basic network scanning techniques.	8.6	More Details
CVE-2025-59088	If kdcproxy receives a request for a realm which does not have server addresses defined in its configuration, by default, it will query SRV records in the DNS zone matching the requested realm name. This creates a server-side request forgery vulnerability, since an attacker could send a request for a realm matching a DNS zone where they created SRV records pointing to arbitrary ports and hostnames (which may resolve to loopback or internal IP addresses). This vulnerability can be exploited to probe internal network topology and firewall rules, perform port scanning, and exfiltrate data. Deployments where the "use_dns" setting is explicitly set to false are not affected.	8.6	More Details
CVE-2025-9317	The vulnerability, if exploited, could allow a miscreant with read access to Edge Project files or Edge Offline Cache files to reverse engineer Edge users' app-native or Active Directory passwords through computational brute-forcing of weak hashes.	8.4	More Details
CVE-2025-60696	A stack-based buffer overflow vulnerability exists in the makeRequest.cgi binary of Linksys RE7000 routers (Firmware FW_v2.0.15_211230_1012). The arplookup function parses lines from /proc/net/arp using sscanf("%16s ... %18s ..."), storing results into buffers v6 (12 bytes) and v7 (20 bytes). Since the format specifiers allow up to 16 and 18 bytes respectively, oversized input can overflow the buffers, resulting in stack corruption. Local attackers controlling /proc/net/arp contents can exploit this issue to cause denial of service or potentially execute arbitrary code.	8.4	More Details
CVE-2025-60692	A stack-based buffer overflow vulnerability exists in the libshared.so library of Cisco Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz). The functions get_mac_from_ip and get_ip_from_mac use sscanf with overly permissive "%100s" format specifiers to parse entries from /proc/net/arp into fixed-size buffers (v6: 50 bytes, v7 sub-arrays: 50 bytes). This allows local attackers controlling the contents of /proc/net/arp to overflow stack buffers, leading to memory corruption, denial of service, or potential arbitrary code execution.	8.4	More Details

CVE-2025-55034	General Industrial Controls Lynx+ Gateway is vulnerable to a weak password requirement vulnerability, which may allow an attacker to execute a brute-force attack resulting in unauthorized access and login.	8.2	More Details
CVE-2025-36236	IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 NIM server (formerly known as NIM master) service (nimesis) could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request to write arbitrary files on the system.	8.2	More Details
CVE-2025-65001	Fujitsu fbiosdrv.sys before 2.5.0.0 allows an attacker to potentially affect system confidentiality, integrity, and availability.	8.2	More Details
CVE-2025-12974	The Gravity Forms plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the legacy chunked upload mechanism in all versions up to, and including, 2.9.21.1. This is due to the extension blacklist not including .phar files, which can be uploaded through the chunked upload mechanism. This makes it possible for unauthenticated attackers to upload executable .phar files and achieve remote code execution on the server, granted they can discover or enumerate the upload path. In order for an attacker to achieve RCE, the web server needs to be set up to process .phar file as PHP via file handler mapping or similar.	8.1	More Details
CVE-2025-12528	The Pie Forms for WP plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.6 via the format_classic function. This is due to insufficient file type validation where the validate_classic method validates file extensions and sets error messages but does not prevent the file upload process from continuing. This makes it possible for unauthenticated attackers to upload files with dangerous extensions such as PHP, which makes remote code execution possible. In order to exploit this vulnerability, the attacker needs to guess the directory in which the file is placed (which is a somewhat predictable hash). In addition to that, the file name is generated using a secure hash method, limiting the exploitability of this vulnerability.	8.1	More Details
CVE-2025-63916	MyScreenTools v2.2.1.0 contains a critical OS command injection vulnerability in the GIF compression tool. The application fails to properly sanitize user-supplied file paths before passing them to cmd.exe, allowing attackers to execute arbitrary system commands with the privileges of the user running the application. The vulnerability exists in the CMD() function within GIFSicleTool\Form_gif_sicle_tool.cs, which constructs shell commands by concatenating unsanitized user input (file paths) and executes them via cmd.exe.	8.1	More Details
CVE-2025-8855	Authorization Bypass Through User-Controlled Key, Weak Password Recovery Mechanism for Forgotten Password, Authentication Bypass by Assumed-Immutable Data vulnerability in Optimus Software Brokerage Automation allows Exploiting Trust in Client, Authentication Bypass, Manipulate Registry Information.This issue affects Brokerage Automation: before 1.1.71.	8.1	More Details
CVE-2025-62406	Piwigo is a full featured open source photo gallery application for the web. In Piwigo 15.6.0, using the password reset function allows sending a password-reset URL by entering an existing username or email address. However, the hostname used to construct this URL is taken from the HTTP request's Host header and is not validated at all. Therefore, an attacker can send a password-reset URL with a modified hostname to an existing user whose username or email the attacker knows or guesses. This issue has been patched in version 15.7.0.	8.1	More Details
CVE-2025-13282	TenderDocTransfer developed by Chunghwa Telecom has a Arbitrary File Delete vulnerability. The application sets up a simple local web server and provides APIs for communication with the target website. Due to the lack of CSRF protection in the APIs, unauthenticated remote attackers could use these APIs through phishing. Additionally, one of the APIs contains an Absolute Path Traversal vulnerability, allowing attackers to delete arbitrary files on the user's system.	8.1	More Details
CVE-2025-64741	Improper authorization handling in Zoom Workplace for Android before version 6.5.10 may allow an unauthenticated user to conduct an escalation of privilege via network access.	8.1	More Details
CVE-2025-62484	Inefficient regular expression complexity in certain Zoom Workplace Clients before version 6.5.10 may allow an unauthenticated user to conduct an escalation of privilege via network access.	8.1	More Details
CVE-2025-64403	Apache OpenOffice Calc spreadsheet can contain links to other files, in the form of "external data sources". A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause such links to be loaded without prompt. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue.	8.1	More Details
CVE-2025-	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. In Vega prior to version 6.2.0, applications meeting 2 conditions are at risk of arbitrary JavaScript code execution, even if "safe mode" expressionInterpreter is used. They are vulnerable if they use `vega` in an application that attaches `vega` library and a `vega.View` instance similar to the Vega Editor to the global `window` and if they allow user-defined Vega `JSON` definitions (vs JSON that was is only provided through source code). Patches are available in the following Vega applications. If using the latest Vega line (6.x), upgrade to `vega` `6.2.0` / `vega-expression` `6.1.0` / `vega-interpreter` `2.2.1` (if using AST	8.1	More Details

59840	evaluator mode). If using Vega in a non-ESM environment, upgrade to `vega-expression` `5.2.1` / `1.2.1` (if using AST evaluator mode). Some workarounds are available. Do not attach `vega` View instances to global variables, and do not attach `vega` to the global window. These practices of attaching the vega library and View instances may be convenient for debugging, but should not be used in production or in any situation where vega/vega-lite definitions could be provided by untrusted parties.		
CVE-2025-36357	IBM Planning Analytics Local 2.1.0 through 2.1.14 could allow a remote authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request containing absolute path sequences to view, read, or write arbitrary files on the system.	8.0	More Details
CVE-2025-48593	In bta_hf_client_cb_init of bta_hf_client_main.cc, there is a possible remote code execution due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.0	More Details
CVE-2025-46369	Dell Alienware Command Center 6.x (AWCC), versions prior to 6.10.15.0, contains an Insecure Temporary File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Privilege Escalation.	7.8	More Details
CVE-2025-13131	A vulnerability was found in Sonarr 4.0.15.2940. The impacted element is an unknown function of the file C:\ProgramData\Sonarr\bin\Sonarr.Console.exe of the component Service. Performing manipulation results in incorrect default permissions. The attack is only possible with local access. The vendor confirms this vulnerability but classifies it as a "low severity issue due to the default service user being used as it would either require someone to intentionally change the service to a highly privileged account or an attacker would need an admin level account". It is planned to fix this issue in the next major release v5.	7.8	More Details
CVE-2025-13130	A vulnerability has been found in Radarr 5.28.0.10274. The affected element is an unknown function of the file C:\ProgramData\Radarr\bin\Radarr.Console.exe of the component Service. Such manipulation leads to incorrect default permissions. The attack can only be performed from a local environment. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2025-33183	NVIDIA Isaac-GR00T for all platforms contains a vulnerability in a Python component, where an attacker could cause a code injection issue. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-46367	Dell Alienware Command Center 6.x (AWCC), versions prior to 6.10.15.0, contain a Detection of Error Condition Without Action vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary Code Execution.	7.8	More Details
CVE-2025-33184	NVIDIA Isaac-GR00T for all platforms contains a vulnerability in a Python component, where an attacker could cause a code injection issue. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-11797	A maliciously crafted DWG file, when parsed through Autodesk 3ds Max, can force a Use-After-Free vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-37155	A vulnerability in the SSH restricted shell interface of the network management services allows improper access control for authenticated read-only users. If successfully exploited, this vulnerability could allow an attacker with read-only privileges to gain administrator access on the affected system.	7.8	More Details
CVE-2025-40936	A vulnerability has been identified in PS/IGES Parasolid Translator Component (All versions < V29.0.258). The affected applications contains an out of bounds read vulnerability while parsing specially crafted IGS files. This could allow an attacker to crash the application or execute code in the context of the current process. (ZDI-CAN-26755)	7.8	More Details
CVE-2025-47761	An Exposed IOCTL with Insufficient Access Control vulnerability [CWE-782] in Fortinet FortiClientWindows 7.4.0 through 7.4.3, FortiClientWindows 7.2.0 through 7.2.9 may allow an authenticated local user to execute unauthorized code via fortips driver. Success of the attack would require bypassing the Windows memory protections such as Heap integrity and HSP. In addition, it requires a valid and running VPN IPSec connection.	7.8	More Details
CVE-2025-46373	A Heap-based Buffer Overflow vulnerability [CWE-122] in Fortinet FortiClientWindows 7.4.0 through 7.4.3, FortiClientWindows 7.2.0 through 7.2.8 may allow an authenticated local IPSec user to execute arbitrary code or commands via "fortips_74.sys". The attacker would need to bypass the Windows heap integrity protections	7.8	More Details
CVE-2025-11795	A maliciously crafted JPG file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-64293	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Golemiq 0 Day Analytics allows SQL Injection.This issue affects 0 Day Analytics: from n/a through 4.0.0.	7.6	More Details
CVE-	A Reflected Cross Site Scripting (XSS) vulnerability was found in the Application Server of Desktop Alert		More

2025-54346	PingAlert version 6.1.0.11 to 6.1.1.2 which allows an attacker to hijack user's browser, capturing sensitive information.	7.6	Details
CVE-2025-12633	The Booking Calendar | Appointment Booking | Bookit plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the '/wp-json/bookit/v1/commerce/stripe/return' REST API Endpoint in all versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to connect their Stripe account and receive payments.	7.5	More Details
CVE-2025-63891	Information Disclosure in web-accessible backup file in SourceCodester Simple Online Book Store System allows a remote unauthenticated attacker to disclose full database contents (including schema and credential hashes) via an unauthenticated HTTP GET request to /obs/database/obs_db.sql.	7.5	More Details
CVE-2025-53843	A stack-based buffer overflow in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions allows attacker to execute unauthorized code or commands via specially crafted packets	7.5	More Details
CVE-2025-65073	OpenStack Keystone before 26.0.1, 27.0.0, and 28.0.0 allows a /v3/ec2tokens or /v3/s3tokens request with a valid AWS Signature to provide Keystone authorization.	7.5	More Details
CVE-2025-12482	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to SQL Injection via the 'search' parameter in all versions up to, and including, 1.2.35 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-63800	The password change endpoint in Open Source Point of Sale 3.4.1 allows users to set their account password to an empty string due to missing server-side validation. When an authenticated user omits or leaves the `password` and `repeat_password` parameters empty in the password change request, the backend still returns a successful response and sets the password to an empty string. This effectively disables authentication and may allow unauthorized access to user or administrative accounts.	7.5	More Details
CVE-2025-59780	General Industrial Controls Lynx+ Gateway is missing critical authentication in the embedded web server which could allow an attacker to send GET requests to obtain sensitive device information.	7.5	More Details
CVE-2025-12048	An arbitrary file upload vulnerability was reported in the Lenovo Scanner Pro client during an internal security assessment that could allow remote code execution or unauthorized control of the affected system.	7.5	More Details
CVE-2025-10495	A potential vulnerability was reported in the Lenovo PC Manager, Lenovo App Store, Lenovo Browser, and Lenovo Legion Zone client applications that, under certain conditions, could allow an attacker on the same logical network to execute arbitrary code.	7.5	More Details
CVE-2025-47913	SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.	7.5	More Details
CVE-2025-63929	A null pointer dereference vulnerability exists in airpig2011 IEC104 thru Commit be6d841 (2019-07-08). When multiple threads enqueue elements concurrently via IEC10X_PrioEnQueue, the function may dereference a null or freed queue pointer, resulting in a segmentation fault and potential denial-of-service.	7.5	More Details
CVE-2024-47866	Ceph is a distributed object, block, and file storage platform. In versions up to and including 19.2.3, using the argument `x-amz-copy-source` to put an object and specifying an empty string as its content leads to the RGW daemon crashing, resulting in a DoS attack. As of time of publication, no known patched versions exist.	7.5	More Details
CVE-2025-65002	Fujitsu / Fsas Technologies iRMC S6 on M5 before 1.37S mishandles Redfish/WebUI access if the length of a username is exactly 16 characters.	7.5	More Details
CVE-2025-63811	An issue was discovered in dvsekhvalnov jose2go 1.5.0 thru 1.7.0 allowing an attacker to cause a Denial-of-Service (DoS) via crafted JSON Web Encryption (JWE) token with an exceptionally high compression ratio.	7.5	More Details
CVE-2025-13033	A vulnerability was identified in the email parsing library due to improper handling of specially formatted recipient email addresses. An attacker can exploit this flaw by crafting a recipient address that embeds an external address within quotes. This causes the application to misdirect the email to the attacker's external address instead of the intended internal recipient. This could lead to a significant data leak of sensitive information and allow an attacker to bypass security filters and access controls.	7.5	More Details
CVE-2025-63955	A Cross-Site Request Forgery (CSRF) vulnerability in the manage-students.php component of PHPGurukul Student Record System v3.2 allows an attacker to trick an authenticated administrator into submitting a forged request. This leads to the unauthorized deletion of user accounts, causing a Denial of Service (DoS).	7.5	More Details

CVE-2025-62765	General Industrial Controls Lynx+ Gateway is vulnerable to a cleartext transmission vulnerability that could allow an attacker to observe network traffic to obtain sensitive information, including plaintext credentials.	7.5	More Details
CVE-2025-36118	IBM Storage Virtualize 8.4, 8.5, 8.7, and 9.1 IKEv1 implementation allows remote attackers to obtain sensitive information from device memory via a Security Association (SA) negotiation request.	7.5	More Details
CVE-2025-55796	The openml/openml.org web application version v2.0.20241110 uses predictable MD5-based tokens for critical user workflows such as signup confirmation, password resets, email confirmation resends, and email change confirmation. These tokens are generated by hashing the current timestamp formatted as "%d %H:%M:%S" without incorporating any user-specific data or cryptographic randomness. This predictability allows remote attackers to brute-force valid tokens within a small time window, enabling unauthorized account confirmation, password resets, and email change approvals, potentially leading to account takeover.	7.5	More Details
CVE-2025-64740	Improper verification of cryptographic signature in the installer for Zoom Workplace VDI Client for Windows may allow an authenticated user to conduct an escalation of privilege via local access.	7.5	More Details
CVE-2025-13046	Bacteriology Laboratory Reporting System developed by ViewLead Technology has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2025-64308	The Brightpick Mission Control web application exposes hardcoded credentials in its client-side JavaScript bundle.	7.5	More Details
CVE-2025-64756	Glob matches files using patterns the shell uses. Starting in version 10.2.0 and prior to versions 10.5.0 and 11.1.0, the glob CLI contains a command injection vulnerability in its -c/--cmd option that allows arbitrary command execution when processing files with malicious names. When glob -c <command> <patterns> are used, matched filenames are passed to a shell with shell: true, enabling shell metacharacters in filenames to trigger command injection and achieve arbitrary code execution under the user or CI account privileges. This issue has been patched in versions 10.5.0 and 11.1.0.	7.5	More Details
CVE-2025-13047	Bacteriology Laboratory Reporting System developed by ViewLead Technology has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2025-58410	Software installed and run as a non-privileged user may conduct improper GPU system calls to gain write permissions to memory buffers exported as read-only. This is caused by improper handling of the memory protections for the buffer resource.	7.5	More Details
CVE-2025-12903	The Payment Plugins Braintree For WooCommerce plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the wc-braintree/v1/3ds/vaulted_nonce REST API endpoint in all versions up to, and including, 3.2.78. This is due to the endpoint being registered with permission_callback set to __return_true and processing user-supplied token IDs without verifying ownership or authentication. This makes it possible for unauthenticated attackers to retrieve payment method nonces for any stored payment token in the system, which can be used to create fraudulent transactions, charge customer credit cards, or attach payment methods to other subscriptions.	7.5	More Details
CVE-2025-64401	Apache OpenOffice documents can contain links. A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. In the affected versions of Apache OpenOffice, documents that used "floating frames" linked to external files would load the contents of those frames without prompting the user for permission to do so. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue. The LibreOffice suite reported this issue as CVE-2023-2255	7.5	More Details
CVE-2025-9982	A vulnerability exists in QuickCMS version 6.8 where sensitive admin credentials are hardcoded in a configuration file and stored in plaintext. This flaw allows attackers with access to the source code or the server file system to retrieve authentication details, potentially leading to privilege escalation. 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.	7.5	More Details
CVE-2025-56527	Plaintext password storage in Kotaemon 0.11.0 in the client's localStorage.	7.5	More Details
CVE-2025-60694	A stack-based buffer overflow exists in the validate_static_route function of the httpd binary on Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz). The function improperly concatenates user-supplied CGI parameters (route_ipaddr_0~3, route_netmask_0~3, route_gateway_0~3) into fixed-size buffers (v6, v10, v14) without proper bounds checking. Remote attackers can exploit this vulnerability via specially crafted HTTP requests to execute arbitrary code or cause denial of service without authentication.	7.5	More Details

CVE-2025-64404	Apache OpenOffice documents can contain links to other files. A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. In the affected versions of Apache OpenOffice, documents that used background fill images, or bullet images, linked to external files would load the contents of those files without prompting the user for permission to do so. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue.	7.5	More Details
CVE-2025-64405	Apache OpenOffice documents can contain links. A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. In the affected versions of Apache OpenOffice, Calc spreadsheet containing DDE links to external files would load the contents of those files without prompting the user for permission to do so. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue.	7.5	More Details
CVE-2025-64076	Multiple vulnerabilities exist in cbor2 through version 5.7.0 in the decode_definite_long_string() function of the C extension decoder (source/decoder.c): (1) Integer Underflow Leading to Out-of-Bounds Read (CWE-191, CWE-125): An incorrect variable reference and missing state reset in the chunk processing loop causes buffer_length to not be reset to zero after UTF-8 character consumption. This results in subsequent chunk_length calculations producing negative values (e.g., chunk_length = 65536 - buffer_length), which are passed as signed integers to the read() method, potentially triggering unlimited read operations and resource exhaustion. (2) Memory Leak via Missing Reference Count Release (CWE-401): The main processing loop fails to release Python object references (Py_DECREF) for chunk objects allocated in each iteration. For CBOR strings longer than 65536 bytes, this causes cumulative memory leaks proportional to the payload size, enabling memory exhaustion attacks through repeated processing of large CBOR payloads. Both vulnerabilities can be exploited remotely without authentication by sending specially-crafted CBOR data containing definite-length text strings with multi-byte UTF-8 characters positioned at 65536-byte chunk boundaries. Successful exploitation results in denial of service through process crashes (CBORDecodeEOF exceptions) or memory exhaustion. The vulnerabilities affect all applications using cbor2's C extension to process untrusted CBOR data, including web APIs, IoT data collectors, and message queue processors. Fixed in commit 851473490281f82d82560b2368284ef33cf6e8f9 pushed with released version 5.7.1.	7.5	More Details
CVE-2025-37161	A vulnerability in the web-based management interface of affected products could allow an unauthenticated remote attacker to cause a denial of service. Successful exploitation could allow an attacker to crash the system, preventing it from rebooting without manual intervention and disrupting network operations.	7.5	More Details
CVE-2025-58413	A stack-based buffer overflow in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0 all versions, FortiSASE 25.3.b allows attacker to execute unauthorized code or commands via specially crafted packets	7.5	More Details
CVE-2025-12955	The Live sales notification for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.3.39. This is due to the "getOrders" function lacking proper authorization and capability checks when the plugin is configured to display recent order information. This makes it possible for unauthenticated attackers to extract sensitive customer information including buyer first names, city, state, country, purchase time and date, and product details.	7.5	More Details
CVE-2025-13165	EasyFlow GP developed by Digiwin has a Denial of service vulnerability, allowing unauthenticated remote attackers to send specific requests that result in denial of web service.	7.5	More Details
CVE-2025-11700	N-central versions < 2025.4 are vulnerable to an XML External Entities injection leading to information disclosure	7.5	More Details
CVE-2024-7017	Inappropriate implementation in DevTools in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2025-54345	An issue was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2. Sensitive Information is exposed to an Unauthorized Actor.	7.5	More Details
CVE-2025-12765	pgAdmin <= 9.9 is affected by a vulnerability in the LDAP authentication mechanism allows bypassing TLS certificate verification.	7.5	More Details
CVE-2025-13161	IQ-Support developed by IQ Service International has an Arbitrary File Read vulnerability, allowing unauthenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2025-12764	pgAdmin <= 9.9 is affected by an LDAP injection vulnerability in the LDAP authentication flow that allows an attacker to inject special LDAP characters in the username, causing the DC/LDAP server and the client to process an unusual amount of data DOS.	7.5	More Details

CVE-2024-9126	Use after free in Internals in Google Chrome on iOS prior to 127.0.6533.88 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a series of curated UI gestures. (Chromium security severity: Medium)	7.5	More Details
CVE-2025-63667	Incorrect access control in SIMICAM v1.16.41-20250725, KEVIEW v1.14.92-20241120, ASECAM v1.14.10-20240725 allows attackers to access sensitive API endpoints without authentication.	7.5	More Details
CVE-2025-41737	Due to webserver misconfiguration an unauthenticated remote attacker is able to read the source of php modules.	7.5	More Details
CVE-2025-64530	Apollo Federation is an architecture for declaratively composing APIs into a unified graph. A vulnerability in versions of Apollo Federation's composition logic prior to 2.9.5, 2.10.4, 2.11.5, and 2.12.1 allowed some queries to Apollo Router to improperly bypass access controls on types/fields. Apollo Federation incorrectly allowed user-defined access control directives on interface types/fields, which could be bypassed by instead querying the implementing object types/fields in Apollo Router via inline fragments, for example. A fix to versions 2.9.5, 2.10.4, 2.11.5, and 2.12.1 of composition logic in Federation now disallows interfaces types and fields to contain user-defined access control directives. Some workarounds are available. Users of Apollo Rover with an unpatched composition version or are using the Apollo Studio build pipeline with Federation version 2.8 or below should manually copy the access control requirements on interface types/fields to each implementing object type/field where appropriate. Do not remove those access control requirements from the interface types/fields, as unpatched Apollo Composition will not automatically generate them in the supergraph schema. Customers not using Apollo Router access control features (`@authenticated`, `@requiresScopes`, or `@policy` directives) or not specifying access control requirements on interface types/fields are not affected and do not need to take action.	7.5	More Details
CVE-2025-64511	MaxKB is an open-source AI assistant for enterprise. In versions prior to 2.3.1, a user can access internal network services such as databases through Python code in the tool module, although the process runs in a sandbox. Version 2.3.1 fixes the issue.	7.4	More Details
CVE-2025-58407	Kernel or driver software installed on a Guest VM may post improper commands to the GPU Firmware to exploit a TOCTOU race condition and trigger a read and/or write of data outside the allotted memory escaping the virtual machine.	7.4	More Details
CVE-2025-13235	A vulnerability was determined in itsourcecode Inventory Management System 1.0. This affects an unknown function of the file /admin/login.php. Executing manipulation of the argument user_email can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-13272	A vulnerability was identified in Campcodes School Fees Payment Management System 1.0. Affected is an unknown function of the file /manage_course.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-13241	A flaw has been found in code-projects Student Information System 2.0. This vulnerability affects unknown code of the file /index.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-13299	A flaw has been found in itsourcecode Web-Based Internet Laboratory Management System 1.0. This impacts an unknown function of the file /user/controller.php. Executing manipulation can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	7.3	More Details
CVE-2025-13297	A security vulnerability has been detected in itsourcecode Web-Based Internet Laboratory Management System 1.0. The impacted element is an unknown function of the file /course/controller.php. Such manipulation leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13262	A vulnerability was determined in lsfusion platform up to 6.1. Affected by this vulnerability is the function UploadFileRequestHandler of the file platform/web-client/src/main/java/lsfusion/http/controller/file/UploadFileRequestHandler.java. Executing manipulation of the argument sid can lead to path traversal. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-13257	A security vulnerability has been detected in itsourcecode Inventory Management System 1.0. The affected element is an unknown function of the file /admin/user/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13248	A weakness has been identified in SourceCodester Patients Waiting Area Queue Management System 1.0. The impacted element is an unknown function of the file /php/api_patient_schedule.php. This manipulation of the argument appointmentID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details

CVE-2025-13121	A security vulnerability has been detected in cameasy Liketea 1.0.0. Impacted is the function list of the file laravel/app/Http/Controllers/Front/StoreController.php of the component API Endpoint. Such manipulation of the argument lng/lat leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13300	A vulnerability has been found in itsourcecode Web-Based Internet Laboratory Management System 1.0. Affected is an unknown function of the file /settings/controller.php. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-13298	A vulnerability was detected in itsourcecode Web-Based Internet Laboratory Management System 1.0. This affects an unknown function of the file /enrollment/controller.php. Performing manipulation results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-60697	A command injection vulnerability exists in the D-Link DIR-882 Router firmware DIR882A1_FW102B02 within the `prog.cgi` and `rc` binaries. The `sub_4438A4` function in `prog.cgi` stores user-supplied DDNS parameters (`ServerAddress` and `Hostname`) in NVRAM via `nvram_safe_set`. These values are later retrieved in the `start_DDNS_ipv4` function of `rc` using `nvram_safe_get` and concatenated into DDNS shell commands executed via `twsystem()` without proper sanitization. Partial string comparison is performed but is insufficient to prevent command injection. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary commands on the device through specially crafted HTTP requests to the router's web interface.	7.3	More Details
CVE-2025-13291	A vulnerability was found in Campcodes Supplier Management System 1.0. This affects an unknown part of the file /manufacturer/confirm_order.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-60698	A command injection vulnerability exists in the D-Link DIR-882 Router firmware DIR882A1_FW102B02 within the `prog.cgi` and `rc` binaries. The `sub_432F60` function in `prog.cgi` stores user-supplied `SetSysLogSettings/IPAddress` values in NVRAM via `nvram_safe_set("SysLogRemote_IPAddress", ...)`. These values are later retrieved in the `sub_448DCC` function of `rc` using `nvram_safe_get` and concatenated into a shell command executed via `twsystem()` without any sanitization. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary commands on the device through specially crafted HTTP requests to the router's web interface.	7.3	More Details
CVE-2025-13247	A security flaw has been discovered in PHPGurukul Tourism Management System 1.0. The affected element is an unknown function of the file /admin/user-bookings.php. The manipulation of the argument uid results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-13276	A vulnerability was detected in g33kyrash Online-Banking-System up to 12dbfa690e5af649fb72d2e5d3674e88d6743455. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument Username results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	7.3	More Details
CVE-2025-13122	A vulnerability was detected in SourceCodester Patients Waiting Area Queue Management System 1.0. The affected element is the function getPatientAppointment of the file /php/api_patient_checkin.php. Performing manipulation of the argument appointmentID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-13277	A flaw has been found in code-projects Nero Social Networking Site 1.0. This issue affects some unknown processing of the file /friendsphoto.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-13233	A vulnerability has been found in itsourcecode Inventory Management System 1.0. The affected element is an unknown function of the file /index.php?q=single-item. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-13252	A vulnerability was found in shsuishang ShopSuite ModulithShop up to 45a99398cec3b7ad7ff9383694f0b53339f2d35a. Affected by this issue is some unknown functionality of the component RSA/OAuth2/Database. The manipulation results in hard-coded credentials. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable.	7.3	More Details
CVE-2025-13285	A vulnerability was identified in itsourcecode Online Voting System 1.0. The affected element is an unknown function of the file /login.php. Such manipulation of the argument Username leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-	A vulnerability was determined in CodeAstro Simple Inventory System 1.0. The impacted element is an unknown function of the file /index.php of the component Login. Executing manipulation of the argument		More

2025-13280	Username can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	Details
CVE-2025-64500	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Symfony's HttpFoundation component defines an object-oriented layer for the HTTP specification. Starting in version 2.0.0 and prior to version 5.4.50, 6.4.29, and 7.3.7, the `Request` class improperly interprets some `PATH_INFO` in a way that leads to representing some URLs with a path that doesn't start with a `/`. This can allow bypassing some access control rules that are built with this `/`-prefix assumption. Starting in versions 5.4.50, 6.4.29, and 7.3.7, the `Request` class now ensures that URL paths always start with a `/`.	7.3	More Details
CVE-2025-11962	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in DivvyDrive Information Technologies Inc. Digital Corporate Warehouse allows Stored XSS.This issue affects Digital Corporate Warehouse: before v.4.8.2.22.	7.3	More Details
CVE-2025-11918	Rockwell Automation Arena® suffers from a stack-based buffer overflow vulnerability. The specific flaw exists within the parsing of DOE files. Local attackers are able to exploit this issue to potentially execute arbitrary code on affected installations of Arena®. Exploiting the vulnerability requires opening a malicious DOE file.	7.3	More Details
CVE-2025-13301	A vulnerability was found in itsourcecode Web-Based Internet Laboratory Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /subject/controller.php. The manipulation results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-13060	A security vulnerability has been detected in SourceCodester Survey Application System 1.0. This affects an unknown function of the file /view_survey.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13169	A security vulnerability has been detected in code-projects Simple Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /add_query_reserve.php. Such manipulation of the argument room_id leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-13237	A security flaw has been discovered in itsourcecode Inventory Management System 1.0. Affected is an unknown function of the file /LogSignModal.PHP. The manipulation of the argument U_USERNAME results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-13240	A vulnerability was detected in code-projects Student Information System 2.0. This affects an unknown part of the file /searchquery.php. Performing manipulation of the argument s results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	7.3	More Details
CVE-2025-13344	A weakness has been identified in SourceCodester Train Station Ticketing System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=login. This manipulation of the argument Username causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-13242	A vulnerability has been found in code-projects Student Information System 2.0. This issue affects some unknown processing of the file /register.php. The manipulation leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-36463	Multiple out-of-bounds read and write vulnerabilities exist in the ControlVault WBDI Driver Broadcom Storage Adapter functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted WinBioControlUnit call can lead to memory corruption. An attacker can issue an api call to trigger this vulnerability. This vulnerability is triggered when submitting a `WinBioControlUnit` call to the StorageAdapter with the ControlCode 4 (`WBIO_USH_ADD_RECORD`) and with an invalid `SendBufferSize`.	7.3	More Details
CVE-2025-36462	Multiple out-of-bounds read and write vulnerabilities exist in the ControlVault WBDI Driver Broadcom Storage Adapter functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted WinBioControlUnit call can lead to memory corruption. An attacker can issue an api call to trigger this vulnerability. This vulnerability is triggered when submitting a `WinBioControlUnit` call to the StorageAdapter with the ControlCode 3 (`WBIO_USH_CREATE_CHALLENGE`) with an invalid `ReceiveBuferSize`.	7.3	More Details
CVE-2025-13203	A weakness has been identified in code-projects Simple Cafe Ordering System 1.0. This vulnerability affects unknown code of the file /addmem.php. Executing manipulation of the argument studentnum can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-36461	Multiple out-of-bounds read and write vulnerabilities exist in the ControlVault WBDI Driver Broadcom Storage Adapter functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted WinBioControlUnit call can lead to memory corruption. An attacker can issue an api call to trigger this vulnerability. This vulnerability is triggered when submitting a `WinBioControlUnit` call to the	7.3	More Details

	StorageAdapter with the ControlCode 0 (`WBIO_USH_GET_TEMPLATE`) and with either and an invalid `ReceiveBuferSize` and/or an invalid `SendBufferSize`.		
CVE-2025-36460	Multiple out-of-bounds read and write vulnerabilities exist in the ControlVault WBDI Driver Broadcom Storage Adapter functionality of Dell ControlVault3 prior to 5.15.14.19 and Dell ControlVault3 Plus prior to 6.2.36.47. A specially crafted WinBioControlUnit call can lead to memory corruption. An attacker can issue an api call to trigger this vulnerability. This vulnerability is triggered when submitting a `WinBioControlUnit` call to the StorageAdapter with the ControlCode 2 (`WBIO_USH_GET_IDENTITY`) with an improper `ReceiveBuferSize` value.	7.3	More Details
CVE-2025-63602	A vulnerability was discovered in Awesome Miner thru 11.2.4 that allows arbitrary read and write to kernel memory and MSRs (such as LSTAR) as an unprivileged user. This is due to the implementation of an insecure version of WinRing0 (1.2.0.5, renamed to IntelliBreeze.Maintenance.Service.sys) that lacks a properly secured DACL, allowing unprivileged users to interact with the driver and, as a result, the kernel. This can result in local privilege escalation, information disclosure, denial of service, and other unspecified impacts.	7.3	More Details
CVE-2025-13323	A security flaw has been discovered in code-projects Simple Pizza Ordering System 1.0. Affected is an unknown function of the file /listorder.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-59118	Unrestricted Upload of File with Dangerous Type vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.03. Users are recommended to upgrade to version 24.09.03, which fixes the issue.	7.3	More Details
CVE-2025-8485	An improper permissions vulnerability was reported in Lenovo App Store that could allow a local authenticated user to execute code with elevated privileges during installation of an application.	7.3	More Details
CVE-2025-13170	A vulnerability was detected in code-projects Simple Online Hotel Reservation System 1.0. This issue affects some unknown processing of the file /admin/edit_account.php. Performing manipulation of the argument admin_id results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-13271	A vulnerability was determined in Campcodes School Fees Payment Management System 1.0. This impacts an unknown function of the file /ajax.php?action=login. This manipulation of the argument Username causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-13063	A flaw has been found in DinukaNavaratna Dee Store 1.0. Affected is an unknown function. Executing manipulation can lead to missing authorization. The attack may be performed from remote. The exploit has been published and may be used. Multiple endpoints are affected.	7.3	More Details
CVE-2025-13204	npm package `expr-eval` is vulnerable to Prototype Pollution. An attacker with access to express eval interface can use JavaScript prototype-based inheritance model to achieve arbitrary code execution. The npm expr-eval-fork package resolves this issue.	7.3	More Details
CVE-2025-13201	A vulnerability was identified in code-projects Simple Cafe Ordering System 1.0. Affected by this issue is some unknown functionality of the file /login.php. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-8076	There is a vulnerability in the Supermicro BMC web function at Supermicro MBD-X13SEDW-F. After logging into the BMC Web server, an attacker can use a specially crafted payload to trigger the Stack buffer overflow vulnerability.	7.2	More Details
CVE-2025-37163	A command injection vulnerability has been identified in the command line interface of the HPE Aruba Networking Airwave Platform. An authenticated attacker could exploit this vulnerability to execute arbitrary operating system commands with elevated privileges on the underlying operating system.	7.2	More Details
CVE-2025-11994	The Easy Email Subscription plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-58034	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.5, FortiWeb 7.4.0 through 7.4.10, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow an authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests or CLI commands.	7.2	More Details
CVE-2025-8727	There is a vulnerability in the Supermicro BMC web function at Supermicro MBD-X13SEDW-F. After logging into the BMC Web server, an attacker can use a specially crafted payload to trigger the Stack buffer overflow vulnerability.	7.2	More Details

CVE-2025-62519	phpMyFAQ is an open source FAQ web application. Prior to version 4.0.14, an authenticated SQL injection vulnerability in the main configuration update functionality of phpMyFAQ allows a privileged user with 'Configuration Edit' permissions to execute arbitrary SQL commands. Successful exploitation can lead to a full compromise of the database, including reading, modifying, or deleting all data, as well as potential remote code execution depending on the database configuration. This issue has been patched in version 4.0.14.	7.2	More Details
CVE-2025-4212	The Checkout Files Upload for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via file uploads in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in image files that will execute whenever a user accesses the injected page.	7.2	More Details
CVE-2025-10686	The Creta Testimonial Showcase WordPress plugin before 1.2.4 is vulnerable to Local File Inclusion. This makes it possible for authenticated attackers, with editor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files.	7.2	More Details
CVE-2025-12904	The SNORDIAN's H5PxAPIkatchu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'insert_data' AJAX endpoint in all versions up to, and including, 0.4.17 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-2025-11620	The Multiple Roles per User plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'mrpu_add_multiple_roles_ui' and 'mrpu_save_multiple_user_roles' functions in all versions up to, and including, 1.0. This makes it possible for authenticated attackers, granted the 'edit_users' capability, to edit any user's role, including promoting users to Administrator and demoting Administrators to lower-privileged roles.	7.2	More Details
CVE-2025-63917	PDFPatcher thru 1.1.3.4663 executable's XML bookmark import functionality does not restrict XML external entity (XXE) references. The application uses .NET's XmlDocument class without disabling external entity resolution, enabling attackers to: Read arbitrary files from the victim's filesystem, exfiltrate sensitive data via out-of-band (OOB) HTTP requests, perform SSRF attacks against internal network resources, or cause a denial of service via entity expansion attacks.	7.1	More Details
CVE-2025-12844	The AI Engine plugin for WordPress is vulnerable to PHP Object Injection via PHAR Deserialization in all versions up to, and including, 3.1.8 via deserialization of untrusted input in the 'rest_simpleTranscribeAudio' and 'rest_simpleVisionQuery' functions. 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 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.	7.1	More Details
CVE-2025-12411	The Premmerce Wholesale Pricing for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'ID' parameter in versions up to, and including, 1.1.10. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber level access and above, to manipulate SQL queries that can be used to extract sensitive information from the database and modify price type display names in the database via the admin-post.php "premmerce_update_price_type" action, causing cosmetic corruption of the admin interface. The 'price_type' parameter of the "premmerce_delete_price_type" is also vulnerable.	7.1	More Details
CVE-2025-13283	TenderDocTransfer developed by Chunghwa Telecom has a Arbitrary File Copy and Paste vulnerability. The application sets up a simple local web server and provides APIs for communication with the target website. Due to the lack of CSRF protection in the APIs, unauthenticated remote attackers could use these APIs through phishing. Additionally, one of the APIs contains an Absolute Path Traversal vulnerability. Attackers can copy arbitrary files on the user's system and paste them into any path, which poses a potential risk of information leakage or could consume hard drive space by copying files in large volumes.	7.1	More Details
CVE-2025-10089	Uncontrolled Search Path Element Vulnerability in Setting and Operation Application for Lighting Control System MILCO.S Setting Application all versions, MILCO.S Setting Application (IR) all versions, MILCO.S Easy Setting Application (IR) all versions, and MILCO.S Easy Switch Application (IR) all versions allows a local attacker to execute malicious code by having installer to load a malicious DLL. However, if the signer name "Mitsubishi Electric Lighting" appears on the "Digital Signatures" tab of the properties for "MILCO.S Lighting Control.exe", the application is a fixed one. This vulnerability only affects when the installer is run, not after installation. If a user downloads directly from Mitsubishi Electric website and installs the affected product, there is no risk of malicious code being introduced.	7.0	More Details
CVE-2025-8386	The vulnerability, if exploited, could allow an authenticated miscreant (with privilege of "aaConfigTools") to tamper with App Objects' help files and persist a cross-site scripting (XSS) injection that when executed by a victim user, can result in horizontal or vertical escalation of privileges. The vulnerability can only be exploited during config-time operations within the IDE component of Application Server. Run-time components and operations are not affected.	6.9	More Details
	The AI Engine plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and		

CVE-2025-8084	including, 3.1.8 via the rest_helpers_create_images function. This makes it possible for authenticated attackers, with Editor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. On Cloud instances, this issue allows for metadata retrieving.	6.8	More Details
CVE-2025-63701	A heap corruption vulnerability exists in the Advantech TP-3250 printer driver's DrvUI_x64_ADVANTECH.dll (v0.3.9200.20789) when DocumentPropertiesW() is called with a valid dmDriverExtra value but an undersized output buffer. The driver incorrectly assumes the output buffer size matches the input buffer size, leading to invalid memory operations and heap corruption. This vulnerability can cause denial of service through application crashes and potentially lead to code execution in user space. Local access is required to exploit this vulnerability.	6.8	More Details
CVE-2025-12763	pgAdmin 4 versions up to 9.9 are affected by a command injection vulnerability on Windows systems. This issue is caused by the use of shell=True during backup and restore operations, enabling attackers to execute arbitrary system commands by providing specially crafted file path input.	6.8	More Details
CVE-2025-55810	A vulnerability was found in Alaga Home Security WiFi Camera 3K (model S-CW2503C-H) with hardware version V03 and firmware version 1.4.2, which allows physical attackers to execute commands as root via script file with a specific name on a SD card.	6.8	More Details
CVE-2025-63892	A vulnerability was determined in SourceCodester Student Grades Management System 1.0. Affected is the function create_classroom of the file /classroom.php of the component My Classrooms Management Page. This manipulation of the argument name/description causes stored cross site scripting.	6.8	More Details
CVE-2025-37156	A platform-level denial-of-service (DoS) vulnerability exists in ArubaOS-CX software. Successful exploitation of this vulnerability could allow an attacker with administrative access to execute specific code that renders the switch non-bootable and effectively non-functional.	6.8	More Details
CVE-2025-60674	A stack buffer overflow vulnerability exists in the D-Link DIR-878A1 router firmware FW101B04.bin in the rc binary's USB storage handling module. The vulnerability occurs when the "Serial Number" field from a USB device is read via sscanf into a 64-byte stack buffer, while fgets reads up to 127 bytes, causing a stack overflow. An attacker with physical access or control over a USB device can exploit this vulnerability to potentially execute arbitrary code on the device.	6.8	More Details
CVE-2025-11538	A vulnerability exists in Keycloak's server distribution where enabling debug mode (--debug <port>) insecurely defaults to binding the Java Debug Wire Protocol (JDWP) port to all network interfaces (0.0.0.0). This exposes the debug port to the local network, allowing an attacker on the same network segment to attach a remote debugger and achieve remote code execution within the Keycloak Java virtual machine.	6.8	More Details
CVE-2025-55055	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	6.8	More Details
CVE-2025-12119	A mongoc_bulk_operation_t may read invalid memory if large options are passed.	6.8	More Details
CVE-2025-64752	grist-core is a spreadsheet hosting server. Prior to version 1.7.7, a user with access to any document on a Grist installation can use a feature for fetching from a URL that is executed on the server. The privileged network access of server-side requests could offer opportunities for attack escalation. This issue is fixed in version 1.7.7. The mitigation was to use the proxy for untrusted fetches intended for such purposes. As a workaround, avoid making http/https endpoints available to an instance running Grist that expose credentials or operate without credentials.	6.8	More Details
CVE-2025-37158	A command injection vulnerability exists in the AOS-CX Operating System. Successful exploitation could allow an authenticated remote attacker to conduct a Remote Code Execution (RCE) on the affected system.	6.7	More Details
CVE-2024-48829	Dell SmartFabric OS10 Software, versions prior to 10.6.1.0, contain an Improper Control of Generation of Code ('Code Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	6.7	More Details
CVE-2025-37157	A command injection vulnerability exists in the AOS-CX Operating System. Successful exploitation could allow an authenticated remote attacker to conduct a Remote Code Execution (RCE) on the affected system.	6.7	More Details
CVE-2025-46362	Dell Alienware Command Center 6.x (AWCC), versions prior to 6.10.15.0, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information Tampering.	6.6	More Details
CVE-2025-46368	Dell Alienware Command Center 6.x (AWCC), versions prior to 6.10.15.0, contains an Insecure Temporary File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	6.6	More Details

CVE-2025-48839	An Out-of-bounds Write vulnerability [CWE-787] in FortiADC 8.0.0, 7.6.0 through 7.6.2, 7.4.0 through 7.4.7, 7.2 all versions, 7.1 all versions, 7.0 all versions, 6.2 all versions may allow an authenticated attacker to execute arbitrary code via specially crafted HTTP requests.	6.6	More Details
CVE-2025-8421	An improper default permission vulnerability was reported in Lenovo Dock Manager that, under certain conditions during installation, could allow an authenticated local user to redirect log files with elevated privileges.	6.6	More Details
CVE-2025-30662	Symlink following in the installer for the Zoom Workplace VDI Plugin macOS Universal installer before version 6.3.14, 6.4.14, and 6.5.10 in their respective tracks may allow an authenticated user to conduct a disclosure of information via network access.	6.6	More Details
CVE-2025-13133	The Simple User Import Export plugin for WordPress is vulnerable to CSV Injection in all versions up to, and including, 1.1.7 via the 'Import/export users' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration	6.6	More Details
CVE-2025-60684	A stack buffer overflow vulnerability exists in the ToToLink LR1200GB (V9.1.0u.6619_B20230130) and NR1800X (V9.1.0u.6681_B20230703) Router firmware within the cstecgi.cgi binary (sub_42F32C function). The web interface reads the "lang" parameter and constructs Help URL strings using sprintf() into fixed-size stack buffers without proper length validation. Maliciously crafted input can overflow these buffers, potentially leading to arbitrary code execution or memory corruption, without requiring authentication.	6.5	More Details
CVE-2025-60683	A command injection vulnerability exists in the ToToLink A720R Router firmware V4.1.5cu.614_B20230630 within the sysconf binary, specifically in the sub_40BFA4 function that handles network interface reinitialization from '/var/system/linux_vlan_reinit'. Input is only partially validated by checking the prefix of interface names, and is concatenated into shell commands executed via system() without escaping. An attacker with write access to this file can execute arbitrary commands on the device.	6.5	More Details
CVE-2025-60682	A command injection vulnerability exists in the ToToLink A720R Router firmware V4.1.5cu.614_B20230630 within the cloudupdate_check binary, specifically in the sub_402414 function that handles cloud update parameters. User-supplied 'magicid' and 'url' values are directly concatenated into shell commands and executed via system() without any sanitization or escaping. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary commands on the device.	6.5	More Details
CVE-2025-52186	Lichess lila before commit 11b4c0fb00f0ffd823246f839627005459c8f05c (2025-06-02) contains a Server-Side Request Forgery (SSRF) vulnerability in the game export API. The players parameter is passed directly to an internal HTTP client without validation, allowing remote attackers to force the server to send HTTP requests to arbitrary URLs	6.5	More Details
CVE-2025-60688	A stack buffer overflow vulnerability exists in the ToToLink LR1200GB (V9.1.0u.6619_B20230130) and NR1800X (V9.1.0u.6681_B20230703) Router firmware within the cstecgi.cgi binary (setDefResponse function). The binary reads the "IpAddress" parameter from a web request and copies it into a fixed-size stack buffer using strcpy() without any length validation. Maliciously crafted input can overflow the buffer, leading to potential arbitrary code execution or memory corruption, without requiring authentication.	6.5	More Details
CVE-2025-64383	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Qode Qi Blocks qi-blocks allows Stored XSS.This issue affects Qi Blocks: from n/a through <= 1.4.3.	6.5	More Details
CVE-2025-60687	An unauthenticated command injection vulnerability exists in the ToToLink LR1200GB Router firmware V9.1.0u.6619_B20230130 within the cstecgi.cgi binary (sub_41EC68 function). The binary reads the "imei" parameter from a web request and verifies only that it is 15 characters long. The parameter is then directly inserted into a system command using sprintf() and executed with system(). Maliciously crafted IMEI input can execute arbitrary commands on the router without authentication.	6.5	More Details
CVE-2025-12937	The ACF Flexible Layouts Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'acf_flm_update_template_with_pasted_layout' function in all versions up to, and including, 1.1.6. This makes it possible for unauthenticated attackers to update custom field values on individual posts and pages.	6.5	More Details
CVE-2025-61623	Reflected cross-site scripting vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.03. Users are recommended to upgrade to version 24.09.03, which fixes the issue.	6.5	More Details
CVE-2025-64525	Astro is a web framework. In Astro versions 2.16.0 up to but excluding 5.15.5 which utilizeon-demand rendering, request headers `x-forwarded-proto` and `x-forwarded-port` are insecurely used, without sanitization, to build the URL. This has several consequences, the most important of which are: middleware-based protected route bypass (only via `x-forwarded-proto`), DoS via cache poisoning (if a CDN is present), SSRF (only via `x-forwarded-proto`), URL pollution (potential SXSS, if a CDN is present), and WAF bypass. Version 5.15.5 contains a patch.	6.5	More Details

CVE-2024-44630	Multiple parameters in register.php in PHPGurukul Student Record System 3.20 are vulnerable to SQL injection. These include: c-full, fname, mname,lname, gname, ocp, nation, mobno, email, board1, roll1, pyear1, board2, roll2, pyear2, sub1,marks1, sub2, course-short, income, category, ph, country, state, city, padd, cadd, and gender.	6.5	More Details
CVE-2024-44632	PHPGurukul Student Record System 3.20 is vulnerable to SQL Injection via the id and emailid parameters in password-recovery.php.	6.5	More Details
CVE-2024-44633	PHPGurukul Student Record System 3.20 is vulnerable to SQL Injection via the currentpassword parameter in change-password.php.	6.5	More Details
CVE-2025-55070	Mattermost versions <11 fail to enforce multi-factor authentication on WebSocket connections which allows unauthenticated users to access sensitive information via WebSocket events	6.5	More Details
CVE-2024-44636	PHPGurukul Student Record System 3.20 is vulnerable to SQL Injection via the adminname and aemailid parameters in /admin-profile.php.	6.5	More Details
CVE-2024-44639	PHPGurukul Student Record System 3.20 is vulnerable to SQL Injection via the sub1, sub2, sub3, sub4, and course-short parameters in add-subject.php.	6.5	More Details
CVE-2024-44640	PHPGurukul Student Record System 3.20 is vulnerable to SQL Injection via the course-short, course-full, and cdate parameters in add-course.php.	6.5	More Details
CVE-2024-55016	PHPGurukul Student Record Management System 3.20 is vulnerable to SQL Injection via the id and password parameters in login.php.	6.5	More Details
CVE-2025-54348	A Stored Cross Site Scripting (XSS) vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows an attacker to hijack user’s browser, capturing sensitive information.	6.5	More Details
CVE-2025-64748	Directus is a real-time API and App dashboard for managing SQL database content. A vulnerability in versions prior to 11.13.0 allows authenticated users to search concealed/sensitive fields when they have read permissions. While actual values remain masked (`****`), successful matches can be detected through returned records, enabling enumeration attacks on sensitive data. Version 11.13.0 fixes the issue.	6.5	More Details
CVE-2025-37162	A vulnerability in the command line interface of affected devices could allow an authenticated remote attacker to conduct a command injection attack. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.	6.5	More Details
CVE-2025-47222	Keyfactor SignServer before 7.3.1 has Incorrect Access Control, issue 3 of 3.	6.5	More Details
CVE-2025-63749	pnetlab 5.3.11 is vulnerable to Command Injection via the qemu_options parameter.	6.5	More Details
CVE-2025-60702	A command injection vulnerability exists in the TOTOLINK A950RG Router firmware V5.9c.4592_B20191022_ALL within the `system.so` binary. The `setDiagnosisCfg` function retrieves the `ipDoamin` parameter from user input via `websGetVar` and concatenates it directly into a `ping` system command executed via `CsteSystem()` without any sanitization. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary commands on the device through specially crafted HTTP requests to the router's web interface.	6.5	More Details
CVE-2025-60699	A buffer overflow vulnerability exists in the TOTOLINK A950RG Router firmware V5.9c.4592_B20191022_ALL within the `global.so` binary. The `getSaveConfig` function retrieves the `http_host` parameter from user input via `websGetVar` and copies it into a fixed-size stack buffer (`v13`) using `strcpy()` without performing any length checks. An unauthenticated remote attacker can exploit this vulnerability by sending a specially crafted HTTP request to the router's web interface, potentially leading to arbitrary code execution.	6.5	More Details
CVE-2025-64380	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pluggabl Booster for WooCommerce woocommerce-jetpack allows Stored XSS.This issue affects Booster for WooCommerce: from n/a through <= 7.3.2.	6.5	More Details
CVE-2025-	The Brightpick Internal Logic Control web interface is accessible without requiring user authentication. An unauthorized user could exploit this interface to manipulate robot control functions, including initiating or	6.5	More

64307	halting runners, assigning jobs, clearing stations, and deploying storage totes.		Details
CVE-2025-60676	An unauthenticated command injection vulnerability exists in the D-Link DIR-878A1 router firmware FW101B04.bin. The vulnerability occurs in the 'SetNetworkSettings' functionality of prog.cgi, where the 'IPAddress' and 'SubnetMask' parameters are directly concatenated into shell commands executed via system(). An attacker can exploit this vulnerability remotely without authentication by sending a specially crafted HTTP request, leading to arbitrary command execution on the device.	6.5	More Details
CVE-2025-60673	An unauthenticated command injection vulnerability exists in the D-Link DIR-878A1 router firmware FW101B04.bin. The vulnerability occurs in the 'SetDMZSettings' functionality, where the 'IPAddress' parameter in prog.cgi is stored in NVRAM and later used by librcm.so to construct iptables commands executed via twsystem(). An attacker can exploit this vulnerability remotely without authentication by sending a specially crafted HTTP request, leading to arbitrary command execution on the device.	6.5	More Details
CVE-2025-60672	An unauthenticated command injection vulnerability exists in the D-Link DIR-878A1 router firmware FW101B04.bin. The vulnerability occurs in the 'SetDynamicDNSSettings' functionality, where the 'ServerAddress' and 'Hostname' parameters in prog.cgi are stored in NVRAM and later used by rc to construct system commands executed via twsystem(). An attacker can exploit this vulnerability remotely without authentication by sending a specially crafted HTTP request, leading to arbitrary command execution on the device.	6.5	More Details
CVE-2025-60701	A command injection vulnerability exists in the D-Link DIR-882 Router firmware DIR882A1_FW102B02 within the `prog.cgi` and `rc` binaries. The `sub_433188` function in `prog.cgi` stores user-supplied email configuration parameters (`EmailFrom`, `EmailTo`, `SMTPServerAddress`, `SMTPServerPort`, `AccountName`) in NVRAM via `nvram_safe_set`. These values are later retrieved in the `sub_448FDC` function of `rc` using `nvram_safe_get` and concatenated into shell commands executed via `twsystem()` without sanitization. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary commands on the device through specially crafted HTTP requests to the router's web interface.	6.5	More Details
CVE-2025-60700	A command injection vulnerability exists in the D-Link DIR-882 Router firmware DIR882A1_FW102B02 within the `prog.cgi` and `librcm.so` binaries. The `sub_4455BC` function in `prog.cgi` stores user-supplied `SetDMZSettings/IPAddress` values in NVRAM via `nvram_safe_set("dmz_ipaddr", ...)`. These values are later retrieved in the `DMZ_run` function of `librcm.so` using `nvram_safe_get` and concatenated into `iptables` shell commands executed via `twsystem()` without any sanitization. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary commands on the device through specially crafted HTTP requests to the router's web interface.	6.5	More Details
CVE-2025-60693	A stack-based buffer overflow exists in the get_merge_mac function of the httpd binary on Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz). The function concatenates up to six user-supplied CGI parameters matching <parameter>_0~5 into a fixed-size buffer (a2) without proper bounds checking, appending colon delimiters during concatenation. Remote attackers can exploit this vulnerability via specially crafted HTTP requests to execute arbitrary code or cause denial of service without authentication.	6.5	More Details
CVE-2025-8994	The Project Management, Team Collaboration, Kanban Board, Gantt Charts, Task Manager and More – WP Project Manager plugin for WordPress is vulnerable to time-based SQL Injection via the 'completed_at_operator' parameter in all versions up to, and including, 2.6.26 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-64402	Apache OpenOffice documents can contain links. A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. In the affected versions of Apache OpenOffice, documents that used "OLE objects" linked to external files would load the contents of those files without prompting the user for permission to do so. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue.	6.5	More Details
CVE-2025-64381	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevelop Booking Calendar booking allows Stored XSS.This issue affects Booking Calendar: from n/a through <= 10.14.7.	6.5	More Details
CVE-2025-64259	Missing Authorization vulnerability in Jeroen Schmit Theater for WordPress theatre allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Theater for WordPress: from n/a through <= 0.18.8.	6.5	More Details
CVE-2024-44641	PHPGurukul Small CRM 3.0 is vulnerable to SQL Injection via the oldpass parameter in change-password.php.	6.5	More Details
CVE-2024-44644	PHPGurukul Small CRM 3.0 is vulnerable to SQL Injection via the frm_id and aremark parameters in manage-tickets.php.	6.5	More Details

CVE-2025-63603	A command injection vulnerability exists in the MCP Data Science Server's (reading-plus-ai/mcp-server-data-exploration) 0.1.6 in the safe_eval() function (src/mcp_server_ds/server.py:108). The function uses Python's exec() to execute user-supplied scripts but fails to restrict the __builtins__ dictionary in the globals parameter. When __builtins__ is not explicitly defined, Python automatically provides access to all built-in functions including __import__, exec, eval, and open. This allows an attacker to execute arbitrary Python code with full system privileges, leading to complete system compromise. The vulnerability can be exploited by submitting a malicious script to the run_script tool, requiring no authentication or special privileges.	6.5	More Details
CVE-2025-63512	kishan0725 Hospital Management System/ v4 is vulnerable to SQL Injection in admin-panel1.php, specifically in the deleting doctor logic. The application fails to properly sanitize or parameterize user-supplied input from the demail parameter before incorporating it directly into a dynamic SQL query.	6.5	More Details
CVE-2025-63604	A code injection vulnerability exists in baryhuang/mcp-server-aws-resources-python 0.1.0 that allows remote code execution through insufficient input validation in the execute_query method. The vulnerability stems from the exposure of dangerous Python built-in functions (__import__, getattr, hasattr) in the execution namespace and the direct use of exec() to execute user-supplied code. An attacker can craft malicious queries to execute arbitrary Python code, leading to AWS credential theft (AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY), file system access, environment variable disclosure, and potential system compromise. The vulnerability allows attackers to bypass intended security controls and gain unauthorized access to sensitive AWS resources and credentials stored in the server's environment.	6.5	More Details
CVE-2025-64261	Missing Authorization vulnerability in codepeople Appointment Booking Calendar appointment-booking-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Appointment Booking Calendar: from n/a through <= 1.3.95.	6.5	More Details
CVE-2025-64262	Cross-Site Request Forgery (CSRF) vulnerability in ramon fincken Auto Prune Posts auto-prune-posts allows Cross Site Request Forgery.This issue affects Auto Prune Posts: from n/a through <= 3.0.0.	6.5	More Details
CVE-2025-12089	The Data Tables Generator by Supsystic plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the cleanCache() function in all versions up to, and including, 1.10.45. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	6.5	More Details
CVE-2025-63258	A remote command execution (RCE) vulnerability was discovered in all H3C ERG3/ERG5 series routers and XiaoBei series routers, cloud gateways, and wireless access points (versions R0162P07, UAP700-WPT330-E2265, UAP672-WPT330-R2262, UAP662E-WPT330-R2262P03, WAP611-WPT330-R1348-OASIS, WAP662-WPT330-R2262, WAP662H-WPT330-R2262, USG300V2-WPT330-R2129, MSG300-WPT330-R1350, and MSG326-WPT330-R2129). Attackers are able to exploit this vulnerability via injecting crafted commands into the sessionid parameter.	6.5	More Details
CVE-2024-44664	PHPGurukul Online Shopping Portal 2.0 is vulnerable to SQL Injection via the name, summary, review, quality, price, and value parameters in product-details.php.	6.5	More Details
CVE-2024-44663	PHPGurukul Online Shopping Portal 2.0 is vulnerable to SQL Injection via the product parameter in search-result.php.	6.5	More Details
CVE-2024-44662	PHPGurukul Online Shopping Portal 2.0 is vulnerable to SQL Injection via the username parameter in the admin page.	6.5	More Details
CVE-2025-11454	The Specific Content For Mobile – Customize the mobile version without redirections plugin for WordPress is vulnerable to SQL Injection via the eos_scfm_duplicate_post_as_draft() function in all versions up to, and including, 0.5.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with COntributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2024-44660	PHPGurukul Online Shopping Portal 2.0 is vulnerable to SQL Injection via the fullname, emailid, and contactno parameters in login.php.	6.5	More Details
CVE-2025-33119	IBM QRadar SIEM 7.5 through 7.5.0 UP14 stores user credentials in configuration files in source control which can be read by an authenticated user.	6.5	More Details
CVE-2024-44658	PHPGurukul Complaint Management System 2.0 is vulnerable to SQL Injection via the subcategory and category parameters in subcategory.php.	6.5	More Details

CVE-2025-64271	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes WP Plugin Manager wp-plugin-manager allows Cross Site Request Forgery.This issue affects WP Plugin Manager: from n/a through <= 1.4.7.	6.5	More Details
CVE-2024-44654	PHPGurukul Complaint Management System 2.0 is vulnerable to SQL Injection via the email and mobileno parameters in reset-password.php.	6.5	More Details
CVE-2025-64275	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevelop Booking Manager booking-manager allows Stored XSS.This issue affects Booking Manager: from n/a through <= 2.1.17.	6.5	More Details
CVE-2025-64276	Missing Authorization vulnerability in Ays Pro Survey Maker survey-maker allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Survey Maker: from n/a through <= 5.1.9.4.	6.5	More Details
CVE-2024-44657	PHPGurukul Complaint Management System 2.0 is vulnerable to SQL Injection via the fromdate and todate parameters in between-date-userreport.php.	6.5	More Details
CVE-2024-44653	Kashipara Ecommerce Website 1.0 is vulnerable to SQL Injection via the user_email parameter in user_login.php.	6.5	More Details
CVE-2024-44651	Kashipara Ecommerce Website 1.0 is vulnerable to SQL Injection via the recover_email parameter in user_password_recover.php.	6.5	More Details
CVE-2024-44652	Kashipara Ecommerce Website 1.0 is vulnerable to SQL Injection via the user_email, username, user_firstname, user_lastname, and user_address parameters in user_register.php.	6.5	More Details
CVE-2024-44648	PHPGurukul Small CRM 3.0 is vulnerable to SQL Injection via id and adminremark parameters in quote-details.php.	6.5	More Details
CVE-2025-64369	Missing Authorization vulnerability in codepeople Contact Form Email contact-form-to-email allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contact Form Email: from n/a through <= 1.3.58.	6.5	More Details
CVE-2025-60645	A Cross-Site Request Forgery (CSRF) in xxl-api v1.3.0 allows attackers to arbitrarily add users to the management module via a crafted GET request.	6.5	More Details
CVE-2025-46776	A buffer copy without checking size of input ('classic buffer overflow') in Fortinet FortiExtender 7.6.0 through 7.6.1, FortiExtender 7.4.0 through 7.4.6, FortiExtender 7.2 all versions, FortiExtender 7.0 all versions may allow an authenticated user to execute arbitrary code or commands via crafted CLI commands.	6.4	More Details
CVE-2025-10295	The Angel – Fashion Model Agency WordPress CMS Theme theme for WordPress is vulnerable to Stored Cross-Site Scripting the profile media uploader in all versions up to, and including, 3.2.3 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. This requires the user has access to the edit profile form with the media upload option.	6.4	More Details
CVE-2025-11769	The WordPress Content Flipper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bgcolor' shortcode attribute of the 'flipper_front' shortcode in all versions up to, and including, 0.1. This is 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-2025-8609	The RTMKit Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Accordion Block's attributes in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12962	The Local Syndication plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.5a via the `url` parameter in the `[syndicate_local]` shortcode. This is due to the use of `wp_remote_get()` instead of `wp_safe_remote_get()` which lacks protections against requests to internal/private IP addresses and localhost. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services, scan internal networks, and access resources that should not be accessible from external networks.	6.4	More Details

CVE-2025-12376	The Icon List Block – Add Icon-Based Lists with Custom Styles plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.2.1 via the fs_api_request function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. Only valid JSON objects are rendered in the response.	6.4	More Details
CVE-2025-8605	The Gutenify – Visual Site Builder Blocks & Site Templates. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block attributes in all versions up to, and including, 1.5.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12457	The Enable SVG, WebP, and ICO Upload plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2025-8397	The Save as PDF Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's restpackpdfbutton shortcode in all versions up to, and including, 1.9.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12823	The CSV to SortTable plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'csv' shortcode in all versions up to, and including, 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-2025-12088	The Meta Display Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Meta Display Block in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2025-11868	The everviz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `everviz` shortcode attributes in versions up to, and including, 1.1. This is due to the plugin not properly sanitizing user input or escaping output when building a `<div id=...>` from the `type` and `hash` 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-2025-12691	The Photonic Gallery & Lightbox for Flickr, SmugMug & Others plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's lightbox functionality in all versions up to, and including, 3.21 due to insufficient input sanitization and output escaping on user supplied caption attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.	6.4	More Details
CVE-2025-11267	The VK All in One Expansion Unit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_veu_custom_css' parameter in all versions up to, and including, 9.112.1. This is due to insufficient input sanitization and output escaping on the user-supplied Custom CSS value. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11265	The VK All in One Expansion Unit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vkExUnit_cta_url' and 'vkExUnit_cta_button_text' parameters in all versions up to, and including, 9.112.1. This is due to a logic error in the CTA save function that reads sanitization callbacks from the wrong variable ($custom_field_name instead of $custom_field_options), causing the sanitization to never be applied. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that execute when a user accesses an injected page.",	6.4	More Details
CVE-2025-13123	A flaw has been found in AMTT Hotel Broadband Operation System 1.0. The impacted element is an unknown function of the file /user/portal/get_firstdate.php. Executing manipulation of the argument uid can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13306	A security vulnerability has been detected in D-Link DWR-M920, DWR-M921, DIR-822K and DIR-825M 1.1.5. Impacted is the function system of the file /boafrm/formDebugDiagnosticRun. The manipulation of the argument host leads to command injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-13254	A vulnerability was identified in projectworlds Advanced Library Management System 1.0. This vulnerability affects unknown code of the file /add_member.php. Such manipulation of the argument roll_number leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	6.3	More Details

CVE-2025-13325	A vulnerability was determined in itsourcecode Student Information System 1.0. The affected element is an unknown function of the file /enrollment_edit1.php. Executing manipulation of the argument en_id can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2024-13983	Inappropriate implementation in Lens in Google Chrome on iOS prior to 136.0.7103.59 allowed a remote attacker to perform UI spoofing via a crafted QR code. (Chromium security severity: Low)	6.3	More Details
CVE-2025-13171	A vulnerability was identified in ZZCMS 2023. This impacts an unknown function of the file /admin/wangkan_list.php. Such manipulation of the argument keyword leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-13346	A vulnerability was detected in SourceCodester Train Station Ticketing System 1.0. This affects an unknown part of the file /ajax.php?action=save_station. Performing manipulation of the argument id/station results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-13172	A security flaw has been discovered in CodeAstro Gym Management System 1.0. Affected is an unknown function of the file /admin/view-member-report.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-13303	A vulnerability was determined in code-projects Courier Management System 1.0. Affected by this issue is some unknown functionality of the file /search-edit.php. This manipulation of the argument Consignment causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-13061	A vulnerability was detected in itsourcecode Online Voting System 1.0. This impacts an unknown function of the file /index.php?page=manage_voting. Performing manipulation results in unrestricted upload. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-13345	A security vulnerability has been detected in SourceCodester Train Station Ticketing System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_ticket. Such manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-13059	A weakness has been identified in SourceCodester Alumni Management System 1.0. The impacted element is an unknown function of the file /manage_career.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-13174	A weakness has been identified in rachelos WeRSS we-mp-rss up to 1.4.7. Affected by this vulnerability is the function do_job of the file /rachelos/we-mp-rss/blob/main/jobs/mps.py of the component Webhook Module. Executing manipulation of the argument web_hook_url can lead to server-side request forgery. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-13057	A vulnerability was identified in Campcodes School Fees Payment Management System 1.0. Impacted is an unknown function of the file /ajax.php?action=save_student. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-13347	A flaw has been found in SourceCodester Train Station Ticketing System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=save_user. Executing manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-13253	A vulnerability was determined in projectworlds Advanced Library Management System 1.0. This affects an unknown part of the file /add_librarian.php. This manipulation of the argument Username causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-13290	A vulnerability has been found in code-projects Simple Food Ordering System 1.0. Affected by this issue is some unknown functionality of the file /saveorder.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-13263	A vulnerability was identified in SourceCodester Online Magazine Management System 1.0. Affected by this issue is some unknown functionality of the file /categories.php. The manipulation of the argument c leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-13260	A vulnerability has been found in Campcodes Supplier Management System 1.0. This impacts an unknown function of the file /manufacturer/edit_product.php. Such manipulation of the argument cmbProductUnit leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-	A flaw has been found in Dromara dataCompare up to 1.0.1. The affected element is the function DbConfig of		

2025-13268	the file src/main/java/com/vince/xq/project/system/dbconfig/service/DbconfigServiceImpl.java of the component JDBC URL Handler. Executing manipulation can lead to injection. The attack can be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-13208	A security flaw has been discovered in FantasticLBP Hotels Server up to 67b44df162fab26df209bd5d5d542875fcbec1d0. The impacted element is an unknown function of the file controller/api/hotelList.php. The manipulation of the argument subjectId/cityName 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-2025-13267	A vulnerability was detected in SourceCodester Dental Clinic Appointment Reservation System 1.0. Impacted is an unknown function of the file /success.php. Performing manipulation of the argument username/password results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-13209	A weakness has been identified in bestfeng oa_git_free up to 9.5. This affects the function updateWriteBack of the file yimioa-oa9.5\server\c-flow\src\main\java\com\cloudweb\oa\controller\WorkflowPredefineController.java. This manipulation of the argument writeProp causes xml external entity reference. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-13265	A weakness has been identified in lsfusion platform up to 6.1. This vulnerability affects the function unpackFile of the file server/src/main/java/lsfusion/server/physics/dev/integration/external/to/file/ZipUtils.java. This manipulation causes path traversal. It is possible to initiate the attack remotely.	6.3	More Details
CVE-2025-13264	A security flaw has been discovered in SourceCodester Online Magazine Management System 1.0. This affects an unknown part of the file /view_magazine.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-13234	A vulnerability was found in itsourcecode Inventory Management System 1.0. The impacted element is an unknown function of the file /index.php?q=product. Performing manipulation of the argument PROID results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-13236	A vulnerability was identified in itsourcecode Inventory Management System 1.0. This impacts an unknown function of the file /admin/products/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-13238	A weakness has been identified in Bdtask Flight Booking Software 4. Affected by this vulnerability is an unknown functionality of the file /agent/profile/edit of the component Edit Profile Page. This manipulation 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-2025-13118	A vulnerability was detected in macrozheng mall-swarm and mall up to 1.0.3. Affected by this issue is the function paySuccess of the file /order/paySuccess. The manipulation of the argument orderID results in improper authorization. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-64703	MaxKB is an open-source AI assistant for enterprise. In versions prior to 2.3.1, a user can get sensitive informations by Python code in tool module, although the process run in sandbox. Version 2.3.1 fixes the issue.	6.3	More Details
CVE-2025-13259	A flaw has been found in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /manufacturer/edit_unit.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-13243	A vulnerability was found in code-projects Student Information System 2.0. Impacted is an unknown function of the file /editprofile.php. The manipulation results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-13246	A vulnerability was identified in shsuishang ShopSuite ModulithShop up to 45a99398cec3b7ad7ff9383694f0b53339f2d35a. Impacted is the function JwtAuthenticationFilter of the file src/main/java/com/suisung/shopsuite/common/security/JwtAuthenticationFilter.java. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	6.3	More Details
CVE-	A vulnerability was identified in macrozheng mall-swarm up to 1.0.3. This affects the function updateAttr of		

2025-13114	the file /cart/update/attr. Such manipulation leads to improper authorization. The attack may be performed from remote. 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-2025-13256	A weakness has been identified in projectworlds Advanced Library Management System 1.0. Impacted is an unknown function of the file /borrow.php. Executing manipulation of the argument roll_number can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-13255	A security flaw has been discovered in projectworlds Advanced Library Management System 1.0. This issue affects some unknown processing of the file /book_search.php. Performing manipulation of the argument book_pub/book_title results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-13249	A security vulnerability has been detected in Jiusi OA up to 20251102. This affects an unknown function of the file /OfficeServer?isAjaxDownloadTemplate=false of the component OfficeServer Interface. Such manipulation of the argument FileData leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-13250	A vulnerability was detected in WeiYe-Jing datax-web up to 2.1.2. This impacts the function remove/update/pause/start/triggerJob of the component Job Handler. Performing manipulation results in improper access controls. The attack may be initiated remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-13251	A flaw has been found in WeiYe-Jing datax-web up to 2.1.2. Affected is an unknown function. Executing manipulation can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-13269	A vulnerability has been found in Campcodes School Fees Payment Management System 1.0. The impacted element is an unknown function of the file /ajax.php?action=save_payment. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-13168	A weakness has been identified in ury-erp ury up to 0.2.0. This affects the function overrided_past_order_list of the file ury/ury/api/pos_extend.py. This manipulation of the argument search_term causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited. Upgrading to version 0.2.1 is able to mitigate this issue. Patch name: 063384e0dddfd191847cd2d6524c342cc380b058. It is suggested to upgrade the affected component. The vendor replied and reacted very professional.	6.3	More Details
CVE-2025-13279	A vulnerability was found in code-projects Nero Social Networking Site 1.0. The affected element is an unknown function of the file /profilefriends.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-13273	A security flaw has been discovered in Campcodes School Fees Payment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_payment. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-13287	A weakness has been identified in itsourcecode Online Voting System 1.0. This affects an unknown function of the file /index.php?page=categories. Executing manipulation of the argument id/category can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-13289	A vulnerability was detected in 1000projects Design & Development of Student Database Management System 1.0. Affected is an unknown function of the file /TeacherLogin/Academics/SubjectDetails.php. The manipulation of the argument SubCode results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	6.3	More Details
CVE-2025-20349	A vulnerability in the REST API of Cisco Catalyst Center could allow an authenticated, remote attacker to execute arbitrary commands in a restricted container as the root user. This vulnerability is due to insufficient validation of user-supplied input in REST API request parameters. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to inject arbitrary commands that would then be executed in a restricted container with root privileges. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Observer.	6.3	More Details
CVE-2025-13274	A weakness has been identified in Campcodes School Fees Payment Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php?action=delete_fees. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-	A vulnerability has been found in projectworlds Advanced Library Management System 1.0. Impacted is an unknown function of the file /borrowed_book_search.php. Such manipulation of the argument	6.3	More

13278	datefrom/dateto leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		Details
CVE-2025-13270	A vulnerability was found in Campcodes School Fees Payment Management System 1.0. This affects an unknown function of the file /ajax.php?action=save_course. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-13286	A security flaw has been discovered in itsourcecode Online Voting System 1.0. The impacted element is an unknown function of the file /ajax.php?action=save_user. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-65013	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Prior to version 25.11.0, a reflected cross-site scripting (XSS) vulnerability was identified in the LibreNMS application at the /maps/nodeimage endpoint. The Image Name parameter is reflected in the HTTP response without proper output encoding or sanitization, allowing an attacker to craft a URL that, when visited by a victim, causes arbitrary JavaScript execution in the victim's browser. This issue has been patched in version 25.11.0.	6.2	More Details
CVE-2025-63918	PDFPatcher executable does not validate user-supplied file paths, allowing directory traversal attacks allowing attackers to upload arbitrary files to arbitrary locations.	6.2	More Details
CVE-2025-12406	The Project Honey Pot Spam Trap plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the printAdminPage() function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-12404	The Like-it plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2. This is due to missing or incorrect nonce validation on the likeit_conf() function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-12078	The ArtiBot Free Chat Bot for WebSites plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PostMessage in all versions up to, and including, 1.1.7 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-2025-52331	Cross-site scripting (XSS) vulnerability in the generate report functionality in Rarlab WinRAR 7.11, allows attackers to disclose user information such as the computer username, generated report directory, and IP address. The generate report command includes archived file names without validation in the HTML report, which allows potentially malicious HTML tags to be injected into the report. User interaction is required. User must use the "generate report" functionality and open the report.	6.1	More Details
CVE-2024-44635	PHPGurukul Student Record System 3.20 is vulnerable to Cross Site Scripting (XSS) via adminname and aemailid parameters in /admin-profile.php.	6.1	More Details
CVE-2024-46334	kashipara School Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the formuser and formpassword parameters in /adminLogin.php.	6.1	More Details
CVE-2024-46336	kashipara School Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via /client_user/feedback.php.	6.1	More Details
CVE-2025-12079	The WP Twitter Auto Publish plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PostMessage in all versions up to, and including, 1.7.3 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-2025-63708	Cross-Site Scripting (XSS) vulnerability exists in SourceCodester AI Font Matcher (nid=18425, 2025-10-10) that allows remote attackers to execute arbitrary JavaScript in victims' browsers. The vulnerability occurs in the webfonts API handling mechanism where font family names are not properly sanitized. An attacker can intercept fetch requests to the webfonts endpoint and inject malicious JavaScript payloads through font family names, resulting in session cookie theft, account hijacking, and unauthorized actions performed on behalf of authenticated users. The vulnerability can be exploited by injecting a fetch hook that returns controlled font data containing malicious scripts.	6.1	More Details
CVE-2025-56526	Cross site scripting (XSS) vulnerability in Kotaemon 0.11.0 allowing attackers to execute arbitrary code via a crafted PDF.	6.1	More Details

CVE-2024-42749	Cross Site Scripting vulnerability in Alto CMS v.1.1.13 allows a local attacker to execute arbitrary code via a crafted script.	6.1	More Details
CVE-2025-59480	Mattermost Mobile Apps versions <=2.32.0 fail to verify that SSO redirect tokens originate from the trusted server, which allows a malicious Mattermost instance or on-path attacker to obtain user session credentials via crafted token-in-URL responses	6.1	More Details
CVE-2024-44647	PHPGurukul Small CRM 3.0 is vulnerable to Cross Site Scripting (XSS) via the aremark parameter in manage-tickets.php.	6.1	More Details
CVE-2025-63514	kishan0725 Hospital Management System has a Cross-Site Scripting (XSS) vulnerability in appsearch.php via the email parameter.	6.1	More Details
CVE-2025-63830	CKFinder 1.4.3 is vulnerable to Cross Site Scripting (XSS) in the File Upload function. An attacker can upload a crafted SVG containing active content.	6.1	More Details
CVE-2025-60646	A stored cross-site scripting (XSS) in the Business Line Management module of Xxl-api v1.3.0 attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name parameter.	6.1	More Details
CVE-2025-63419	Cross Site Scripting (XSS) vulnerability in CrushFTP 11.3.6_48. The Web-Based Server has a feature where users can share files, the feature reflects the filename to an emailbody field with no sanitations leading to HTML Injection.	6.1	More Details
CVE-2025-59491	Cross Site Scripting vulnerability in CentralSquare Community Development 19.5.7 via form fields.	6.1	More Details
CVE-2025-64046	OpenRapid RapidCMS 1.3.1 is vulnerable to Cross Site Scripting (XSS) in /system/update-run.php.	6.1	More Details
CVE-2024-44655	PHPGurukul Complaint Management System 2.0 is vulnerable to Cross Site Scripting (XSS) via the search parameter in user-search.php.	6.1	More Details
CVE-2025-20353	A vulnerability in the web-based management interface of Cisco Catalyst Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of the web-based management interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2025-63725	Reflected Cross-Site Scripting (XSS) vulnerability in SVX Portal 2.7A via the id parameter to Recivers.php.	6.1	More Details
CVE-2025-63724	SQL injection (SQL-i) vulnerability in SVX Portal 2.7A via crafted POST request to admin/update_setings.php.	6.0	More Details
CVE-2025-59089	If an attacker causes kdcproxy to connect to an attacker-controlled KDC server (e.g. through server-side request forgery), they can exploit the fact that kdcproxy does not enforce bounds on TCP response length to conduct a denial-of-service attack. While receiving the KDC's response, kdcproxy copies the entire buffered stream into a new buffer on each recv() call, even when the transfer is incomplete, causing excessive memory allocation and CPU usage. Additionally, kdcproxy accepts incoming response chunks as long as the received data length is not exactly equal to the length indicated in the response header, even when individual chunks or the total buffer exceed the maximum length of a Kerberos message. This allows an attacker to send unbounded data until the connection timeout is reached (approximately 12 seconds), exhausting server memory or CPU resources. Multiple concurrent requests can cause accept queue overflow, denying service to legitimate clients.	5.9	More Details
CVE-2025-13081	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection.This issue affects Drupal core: from 8.0.0 before 10.4.9, from 10.5.0 before 10.5.6, from 11.0.0 before 11.1.9, from 11.2.0 before 11.2.8.	5.9	More Details
CVE-2025-12818	Integer wraparound in multiple PostgreSQL libpq client library functions allows an application input provider or network peer to cause libpq to undersize an allocation and write out-of-bounds by hundreds of megabytes. This results in a segmentation fault for the application using libpq. Versions before PostgreSQL 18.1, 17.7,	5.9	More Details

	16.11, 15.15, 14.20, and 13.23 are affected.		
CVE-2025-60695	A stack-based buffer overflow vulnerability exists in the mtk_dut binary of Linksys E7350 routers (Firmware 1.1.00.032). The function sub_4045A8 reads up to 256 bytes from /sys/class/net/%s/address into a local buffer and then copies it into caller-provided buffer a1 using strcpy without boundary checks. Since a1 is often allocated with significantly smaller sizes (20-32 bytes), local attackers controlling the contents of /sys/class/net/%s/address can trigger buffer overflows, leading to memory corruption, denial of service, or potential arbitrary code execution.	5.9	More Details
CVE-2025-64264	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aman Popup addon for Ninja Forms popup-addon-for-ninja-forms allows Stored XSS.This issue affects Popup addon for Ninja Forms: from n/a through <= 3.5.1.	5.9	More Details
CVE-2025-37159	A vulnerability in the web management interface of the AOS-CX OS user authentication service could allow an authenticated remote attacker to hijack an active user session. Successful exploitation may enable the attacker to maintain unauthorized access to the session, potentially leading to the view or modification of sensitive configuration data.	5.8	More Details
CVE-2025-11427	The WP Migrate Lite – WordPress Migration Made Easy plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 2.7.6 via the wpmdb_flush AJAX action. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to obtain information about internal services.	5.8	More Details
CVE-2025-64714	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. Starting in version 1.7.7 and prior to version 2.0.3, an unauthenticated Local File Inclusion exists in the template-switching feature. If `templateselection` is enabled in the configuration, the server trusts the `template` cookie and includes the referenced PHP file. An attacker can read sensitive data or, if they manage to drop a PHP file elsewhere, gain remote code execution. The constructed path of the template file is checked for existence, then included. For PrivateBin project files this does not leak any secrets due to data files being created with PHP code that prevents execution, but if a configuration file without that line got created or the visitor figures out the relative path to a PHP script that directly performs an action without appropriate privilege checking, those might execute or leak information. The issue has been patched in version 2.0.3. As a workaround, set `templateselection = false` (which is the default) in `cfg/conf.php` or remove it entirely	5.8	More Details
CVE-2025-40834	A vulnerability has been identified in Mendix RichText (All versions >= V4.0.0 < V4.6.1). Affected widget does not properly neutralize the input. This could allow an attacker to execute cross-site scripting attacks.	5.7	More Details
CVE-2025-52578	Incorrect Usage of Seeds in Pseudo-Random Number Generator (CWE- 335) vulnerability in the High Sec ELM may allow a sophisticated attacker with physical access, to compromise internal device communications. This issue affects Command Centre Server: 9.30 prior to vCR9.30.251028a (distributed in 9.30.2881 (MR3)), 9.20 prior to vCR9.20.251028a (distributed in 9.20.3265 (MR5)), 9.10 prior to vCR9.10.251028a (distributed in 9.10.4135 (MR8)), all versions of 9.00 and prior.	5.7	More Details
CVE-2025-52457	Observable Timing Discrepancy (CWE-208) in HBUS devices may allow an attacker with physical access to the device to extract device-specific keys, potentially compromising further site security. This issue affects Command Centre Server: 9.30 prior to vCR9.30.251028a (distributed in 9.30.2881 (MR3)), 9.20 prior to vCR9.20.251028a (distributed in 9.20.3265 (MR5)), 9.10 prior to vCR9.10.251028a (distributed in 9.10.4135 (MR8)), all versions of 9.00 and prior.	5.7	More Details
CVE-2025-63745	A NULL pointer dereference vulnerability was discovered in radare2 6.0.5 and earlier within the info() function of bin_ne.c. A crafted binary input can trigger a segmentation fault, leading to a denial of service when the tool processes malformed data.	5.5	More Details
CVE-2025-8404	Stack buffer overflow vulnerability exists in the Supermicro BMC Shared library. An authenticated attacker with access to the BMC exploit stack buffer via a crafted header and achieve arbitrary code execution of the BMC’s firmware operating system.	5.5	More Details
CVE-2025-54660	An active debug code vulnerability in Fortinet FortiClientWindows 7.4.0 through 7.4.3, FortiClientWindows 7.2.0 through 7.2.10, FortiClientWindows 7.0 all versions may allow a local attacker to run the application step by step and retrieve the saved VPN user password	5.5	More Details
CVE-2025-46775	A debug messages revealing unnecessary information vulnerability in Fortinet FortiExtender 7.6.0 through 7.6.1, FortiExtender 7.4.0 through 7.4.6, FortiExtender 7.2 all versions, FortiExtender 7.0 all versions may allow an authenticated user to obtain administrator credentials via debug log commands.	5.5	More Details
CVE-2025-13193	A flaw was found in libvirt. External inactive snapshots for shut-down VMs are incorrectly created as world-readable, making it possible for unprivileged users to inspect the guest OS contents. This results in an information disclosure vulnerability.	5.5	More Details
CVE-	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Prior to version 25.11.0, a boolean-based blind SQL injection vulnerability was identified in the LibreNMS application at the		More

2025-65093	/ajax_output.php endpoint. The hostname parameter is interpolated directly into an SQL query without proper sanitization or parameter binding, allowing an attacker to manipulate the query logic and infer data from the database through conditional responses. This issue has been patched in version 25.11.0.	5.5	Details
CVE-2025-64747	Directus is a real-time API and App dashboard for managing SQL database content. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 11.13.0 that allows users with `upload files` and `edit item` permissions to inject malicious JavaScript through the Block Editor interface. Attackers can bypass Content Security Policy (CSP) restrictions by combining file uploads with iframe srcdoc attributes, resulting in persistent XSS execution. Version 11.13.0 fixes the issue.	5.5	More Details
CVE-2025-55179	Incomplete validation of rich response messages in WhatsApp for iOS prior to v2.25.23.73, WhatsApp Business for iOS v2.25.23.82, and WhatsApp for Mac v2.25.23.83 could have allowed a user to trigger processing of media content from an arbitrary URL on another user’s device. We have not seen evidence of exploitation in the wild.	5.4	More Details
CVE-2025-13097	Inappropriate implementation in DevTools in Google Chrome prior to 136.0.7103.59 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2025-36223	IBM OpenPages 9.0 and 9.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	5.4	More Details
CVE-2025-63291	When processing API requests, the Alteryx server 2022.1.1.42654 and 2024.1 used MongoDB object IDs to uniquely identify the data being requested by the caller. The Alteryx server did not check whether the authenticated user had permission to access the specified MongoDB object ID. By specifying particlar MongoDB object IDs, callers could obtain records for other users without proper authorization. Records retrievable using this attack included administrative API keys and private studio api keys.	5.4	More Details
CVE-2025-64707	Frappe Learning is a learning system that helps users structure their content. Starting in version 2.0.0 and prior to version 2.41.0, when admins revoked a role from the user, the effect was not immediate because of caching. The issue has been fixed in version 2.41.0 by ensuring the cache is cleared after roles are updated.	5.4	More Details
CVE-2025-7711	The The Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.0.3. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	5.4	More Details
CVE-2025-12760	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Email TFA allows Functionality Bypass.This issue affects Email TFA: from 0.0.0 before 2.0.6.	5.4	More Details
CVE-2025-63883	A DOM-based cross-site scripting vulnerability exists in electic-shop v1.0 (Bhabishya-123/E-commerce). The site's client-side JavaScript reads attacker-controlled input (for example, values derived from the URL or page fragment) and inserts it into the DOM via unsafe sinks (innerHTML/insertAdjacentHTML/document.write) without proper sanitization or context-aware encoding. An attacker can craft a malicious URL that, when opened by a victim, causes arbitrary JavaScript to execute in the victim's browser under the electic-shop origin.	5.4	More Details
CVE-2025-12524	The Post Type Switcher plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 4.0.0 due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to modify the post type of arbitrary posts and pages they do not own, including those created by administrators, which can lead to site disruption, broken navigation, and SEO impact.	5.4	More Details
CVE-2025-7623	Stack-based buffer overflow in the SMASH-CLP shell. An authenticated attacker with SSH access to the BMC can exploit a stack buffer overflow via a crafted SMASH command, overwrite the return address and registers, and achieve arbitrary code execution on the BMC firmware operating system	5.4	More Details
CVE-2025-60689	An unauthenticated command injection vulnerability exists in the Start_EPI function of the httpd binary on Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz). The vulnerability occurs because user-supplied CGI parameters (wl_ant, wl_ssid, wl_rate, ttcp_num, ttcp_ip, ttcp_size) are concatenated into system command strings without proper sanitization and executed via wl_exec_cmd. Successful exploitation allows remote attackers to execute arbitrary commands on the device without authentication.	5.4	More Details
CVE-2024-44661	PHPGurukul Online Shopping Portal 2.0 is vulnerable to Cross Site Scripting (XSS) via the quantity parameter in my-cart.php.	5.4	More Details
CVE-2025-	A command injection vulnerability exists in the D-Link DIR-823G router firmware DIR823G_V1.0.2B05_20181207.bin in the timelycheck and sysconf binaries, which process the /var/system/linux_vlan_reinit file. The vulnerability occurs because content read from this file is only partially	5.4	More Details

60671	validated for a prefix and then formatted using vsnprintf() before being executed with system(), allowing an attacker with write access to /var/system/linux_vlan_reinit to execute arbitrary commands on the device.		
CVE-2025-13196	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Open Street Map widget's marker content parameter in all versions up to, and including, 8.3.4. This is due to insufficient input sanitization and output escaping on user-supplied attributes in the render function. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-60675	A command injection vulnerability exists in the D-Link DIR-823G router firmware DIR823G_V1.0.2B05_20181207.bin in the timelycheck and sysconf binaries, which process the /tmp/new_qos.rule configuration file. The vulnerability occurs because parsed fields from the configuration file are concatenated into command strings and executed via system() without any sanitization. An attacker with write access to /tmp/new_qos.rule can execute arbitrary commands on the device.	5.4	More Details
CVE-2025-26391	SolarWinds Observability Self-Hosted XSS Vulnerability. The SolarWinds Platform was susceptible to a XSS vulnerability that affects user-created URL fields. This vulnerability requires authentication from a low-level account.	5.4	More Details
CVE-2025-13117	A security vulnerability has been detected in macrozheng mall-swarm and mall up to 1.0.3. Affected by this vulnerability is the function cancelOrder of the file /order/cancelOrder. The manipulation of the argument orderId leads to improper authorization. The attack can be initiated 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.	5.4	More Details
CVE-2025-7704	Supermicro BMC Insyde SMASH shell program has a stacked-based overflow vulnerability	5.4	More Details
CVE-2025-64084	An authenticated SQL injection vulnerability exists in Cloudlog 2.7.5 and earlier. The vucc_details_ajax function in application/controllers/Awards.php does not properly sanitize the user-supplied Gridsquare POST parameter. This allows a remote, authenticated attacker to execute arbitrary SQL commands by injecting a malicious payload, which is then concatenated directly into a raw SQL query in the vucc_qso_details function.	5.4	More Details
CVE-2025-55073	Mattermost versions 10.11.x <= 10.11.3, 10.5.x <= 10.5.11, 10.12.x <= 10.12.0 fail to validate the relationship between the post being updated and the MSTeams plugin OAuth flow which allows an attacker to edit arbitrary posts via a crafted MSTeams plugin OAuth redirect URL.	5.4	More Details
CVE-2025-12872	The a+HRD and a+HCM developed by aEnrich has a Stored Cross-Site Scripting vulnerability, allowing authenticated remote attackers to upload files containing malicious JavaScript code, which will execute on the client side when a user is tricked into visiting a specific URL.	5.4	More Details
CVE-2025-63645	A stored cross-site scripting (XSS) vulnerability exists in pH7Software pH7-Social-Dating-CMS 17.9.1 in the application's message system. Unsanitized message content submitted by one user is persisted by the server and later rendered in another user's Inbox view without appropriate context-aware encoding. As a result, attacker-controlled content executes in the recipient's browser context when the Inbox message is viewed.	5.4	More Details
CVE-2025-13116	A weakness has been identified in macrozheng mall-swarm and mall up to 1.0.3. Affected is the function cancelUserOrder of the file /order/cancelUserOrder. Executing manipulation of the argument orderId can lead to improper authorization. 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.	5.4	More Details
CVE-2025-11734	The Broken Link Checker by AIOSEO – Easily Fix/Monitor Internal and External links plugin for WordPress is vulnerable to unauthorized post modification due to missing authorization in all versions up to, and including, 1.2.5. This is due to the plugin registering a REST API endpoint that only checks for a broad capability (aioseo_blc_broken_links_page) that is granted to contributor level users, without verifying the user's permission to perform actions on the specific post being targeted. This makes it possible for authenticated attackers, with contributor level access and above, to trash arbitrary posts via the DELETE /wp-json/aioseoBrokenLinkChecker/v1/post endpoint.	5.4	More Details
CVE-2025-64263	Missing Authorization vulnerability in PluginEver WP Content Pilot wp-content-pilot allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Content Pilot: from n/a through <= 2.1.7.	5.4	More Details
CVE-2025-47220	Keyfactor SignServer before 7.3.1 has Incorrect Access Control, issue 1 of 3.	5.3	More Details
CVE-	Apache OpenOffice documents can contain links. A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt. Such links could also be used to transmit system information, such as environment variables or configuration settings. In the affected versions of Apache OpenOffice, documents that used a certain URI scheme linking to		More

2025-64407	external files would load the contents of such files without prompting the user for permission to do so. Such URI scheme allows to include system configuration data, that is not supposed to be transmitted externally. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue. The LibreOffice suite reported this issue as CVE-2024-12426.	5.3	Details
CVE-2025-63829	eProsima Fast-DDS v3.3 and before has an infinite loop vulnerability caused by integer overflow in the Time_t:: fraction() function.	5.3	More Details
CVE-2025-12849	The Contest Gallery plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 28.0.2. This is due to the plugin registering the `cg_check_wp_admin_upload_v10` AJAX action for both authenticated and unauthenticated users without implementing capability checks or nonce verification. This makes it possible for unauthenticated attackers to inject arbitrary WordPress media attachments into galleries and manipulate gallery metadata via the `cg_check_wp_admin_upload_v10` action. It does not enable an attacker to move or upload files.	5.3	More Details
CVE-2025-46215	An Improper Isolation or Compartmentalization vulnerability [CWE-653] in Fortinet FortiSandbox 5.0.0 through 5.0.1, FortiSandbox 4.4.0 through 4.4.7, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may allow an unauthenticated attacker to evade the sandboxing scan via a crafted file.	5.3	More Details
CVE-2025-59669	A use of hard-coded credentials vulnerability in Fortinet FortiWeb 7.6.0, FortiWeb 7.4 all versions, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow an authenticated attacker with shell access to the device to connect to redis service and access its data	5.3	More Details
CVE-2025-12536	The SureForms plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.13.1 via the '_srfm_email_notification' post meta registration. This is due to setting the 'auth_callback' parameter to '__return_true', which allows unauthenticated access to the metadata. This makes it possible for unauthenticated attackers to extract sensitive data including email notification configurations, which frequently contain vendor-provided CRM/help desk dropbox addresses, CC/BCC recipients, and notification templates that can be abused to inject malicious data into downstream systems.	5.3	More Details
CVE-2025-12392	The Cryptocurrency Payment Gateway for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'handle_optin_optout' function in all versions up to, and including, 2.0.22. This makes it possible for unauthenticated attackers to opt in and out of tracking.	5.3	More Details
CVE-2025-12892	The Survey Maker plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the deactivate_plugin_option() function in all versions up to, and including, 5.1.9.4. This makes it possible for unauthenticated attackers to update the ays_survey_maker_upgrade_plugin option.	5.3	More Details
CVE-2025-12979	The Welcart e-Commerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'usces_export' action in all versions up to, and including, 2.11.24. This makes it possible for unauthenticated attackers to access configured payment credentials (ex. PayPal api secret) , as well as business contact details, mail templates, and other operational settings tied to the store.	5.3	More Details
CVE-2025-12377	The Gallery Plugin for WordPress – Envira Photo Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.12.0. This makes it possible for authenticated attackers, with Author-level access and above, to perform multiple actions, such as removing images from arbitrary galleries. The vulnerability was partially patched in version 1.12.0.	5.3	More Details
CVE-2025-64277	Missing Authorization vulnerability in QuantumCloud ChatBot chatbot allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ChatBot: from n/a through <= 7.3.9.	5.3	More Details
CVE-2025-13261	A vulnerability was found in lsfusion platform up to 6.1. Affected is the function DownloadFileRequestHandler of the file web-client/src/main/java/lsfusion/http/controller/file/DownloadFileRequestHandler.java. Performing manipulation of the argument Version results in path traversal. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	5.3	More Details
CVE-2025-62483	Improper removal of sensitive information in certain Zoom Clients before version 6.5.10 may allow an unauthenticated user to conduct a disclosure of information via network access.	5.3	More Details
CVE-2025-13120	A vulnerability has been found in mruby up to 3.4.0. This vulnerability affects the function sort_cmp of the file src/array.c. Such manipulation leads to use after free. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The name of the patch is eb398971bfb43c38db3e04528b68ac9a7ce509bc. It is advisable to implement a patch to correct this issue.	5.3	More Details
CVE-2025-11260	The WP Headless CMS Framework plugin for WordPress is vulnerable to protection mechanism bypass in all versions up to, and including, 1.15. This is due to the plugin only checking for the existence of the Authorization header in a request when determining if the nonce protection should be bypassed. This makes it possible for unauthenticated attackers to access content they should not have access to.	5.3	More Details

CVE-2025-37160	A broken access control (BAC) vulnerability in the web-based management interface could allow an authenticated remote attacker with low privileges to view sensitive information. Successful exploitation of this vulnerability could enable the attacker to disclose sensitive data.	5.3	More Details
CVE-2025-13221	A weakness has been identified in Intelbras UnniTI 24.07.11. The affected element is an unknown function of the file /xml/sistema/usuarios.xml. Executing manipulation of the argument Usuario/Senha can lead to unprotected storage of credentials. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	5.3	More Details
CVE-2025-12681	The Comment Edit Core – Simple Comment Editing plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.0 via the 'ajax_get_comment' function. This makes it possible for unauthenticated attackers to extract sensitive data including user IDs, IP addresses, and email addresses.	5.3	More Details
CVE-2025-64718	js-yaml is a JavaScript YAML parser and dumper. In js-yaml 4.1.0 and below, it's possible for an attacker to modify the prototype of the result of a parsed yaml document via prototype pollution (`__proto__`). All users who parse untrusted yaml documents may be impacted. The problem is patched in js-yaml 4.1.1. Users can protect against this kind of attack on the server by using `node --disable-proto=delete` or `deno` (in Deno, pollution protection is on by default).	5.3	More Details
CVE-2025-13200	A vulnerability was determined in SourceCodester Farm Management System 1.0. Affected by this vulnerability is an unknown functionality. This manipulation causes exposure of information through directory listing. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	5.3	More Details
CVE-2025-13199	A vulnerability was found in code-projects Email Logging Interface 2.0. Affected is an unknown function of the file signup.cpp. The manipulation of the argument Username results in path traversal: '../filedir'. The attack is only possible with local access. The exploit has been made public and could be used.	5.3	More Details
CVE-2025-12891	The Survey Maker plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'ays_survey_show_results' AJAX endpoint in all versions up to, and including, 5.1.9.4. This makes it possible for unauthenticated attackers to view all survey submissions.	5.3	More Details
CVE-2025-13266	A security vulnerability has been detected in wwwlike vlife up to 2.0.1. This issue affects the function create of the file vlife-base/src/main/java/cn/wwwlike/sys/api/SysFileApi.java of the component VLifeApi. Such manipulation of the argument fileName leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2025-6171	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.2 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2 that could have allowed an authenticated attacker with reporter access to view branch names and pipeline details by accessing the packages API endpoint even when repository access was disabled.	5.3	More Details
CVE-2025-13080	Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal Drupal core allows Forceful Browsing.This issue affects Drupal core: from 8.0.0 before 10.4.9, from 10.5.0 before 10.5.6, from 11.0.0 before 11.1.9, from 11.2.0 before 11.2.8.	5.3	More Details
CVE-2025-64370	Missing Authorization vulnerability in YOP YOP Poll yop-poll allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects YOP Poll: from n/a through <= 6.5.38.	5.3	More Details
CVE-2025-12545	The Pixel Manager for WooCommerce – Track Conversions and Analytics, Google Ads, TikTok and more plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.49.2 via the ajax_pmw_get_product_ids() function due to insufficient restrictions on which products can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft products that they should not have access to.	5.3	More Details
CVE-2025-54990	XWiki AdminTools integrates administrative tools for managing a running XWiki instance. Prior to version 1.1, users without admin rights have access to AdminTools.SpammedPages. View rights are not restricted only to admin users for AdminTools.SpammedPages. While no data is visible to non admin users, the page is still accessible. This issue has been patched in version 1.1. A workaround involves setting the view rights for the AdminTools space to be only available for the XWikiAdminGroup.	5.3	More Details
CVE-2025-64753	grist-core is a spreadsheet hosting server. Prior to version 1.7.7, a user with only partial read access to a document could still access endpoints listing hashes for versions of that document and receive a full list of changes between versions, even if those changes contained cells, columns, or tables to which the user was not supposed to have read access. This was fixed in version 1.7.7 by restricting the `/compare` endpoint to users with full read access. As a workaround, remove sensitive document history using the `/states/remove` endpoint. Another possibility is to block the `/compare` endpoint.	5.3	More Details
CVE-2025-13160	IQ-Support developed by IQ Service International has a Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to access specific APIs to obtain sensitive information from the internal network.	5.3	More Details

CVE-2025-13187	A security vulnerability has been detected in Intelbras ICIP 2.0.20. Affected is an unknown function of the file /xml/sistema/acessodeusuario.xml. Such manipulation of the argument NomeUsuario/SenhaAcess leads to unprotected storage of credentials. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2025-12047	A vulnerability was reported in the Lenovo Scanner pro application during an internal security assessment that, under certain circumstances, could allow an attacker on the same logical network to disclose sensitive user files from the application.	5.3	More Details
CVE-2024-45301	Mintty is a terminal emulator for Cygwin, MSYS, and WSL. In versions 2.3.6 through 3.7.4, several escape sequences can cause the mintty process to access a file in a specific path. It is triggered by simply printing them out on bash. An attacker can specify an arbitrary network path, negotiate an ntlm hash out of the victim's machine to an attacker controlled remote host. An attacker can use password cracking tools or NetNTLMv2 hashes to Pass the Hash. Version 3.7.5 fixes the issue.	5.3	More Details
CVE-2025-25236	Omnissa Workspace ONE UEM contains an observable response discrepancy vulnerability. A malicious actor may be able to enumerate sensitive information such as tenant ID and user accounts that could facilitate brute-force, password-spraying or credential-stuffing attacks.	5.3	More Details
CVE-2025-12391	The Restrictions for BuddyPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the handle_optin_optout() function in all versions up to, and including, 1.5.2. This makes it possible for unauthenticated attackers to opt in and out of tracking.	5.3	More Details
CVE-2025-6599	An uncontrolled resource consumption vulnerability in the web server of Zyxel DX3301-T0 firmware version 5.50(ABVY.6.3)C0 and earlier could allow an attacker to perform Slowloris-style denial-of-service (DoS) attacks. Such attacks may temporarily block legitimate HTTP requests and partially disrupt access to the web management interface, while other networking services remain unaffected.	5.3	More Details
CVE-2025-64766	NixOS's Onlyoffice is a software suite that offers online and offline tools for document editing, collaboration, and management. In versions from 22.11 to before 25.05 and versions before Unstable 25.11, a hard-coded secret was used in the NixOS module for the OnlyOffice document server to protect its file cache. An attacker with knowledge of an existing revision ID could use this secret to obtain a document. In practice, an arbitrary revision ID should be hard to obtain. The primary impact is likely the access to known documents from users with expired access. This issue was resolved in NixOS unstable version 25.11 and version 25.05.	5.3	More Details
CVE-2025-47221	Keyfactor SignServer before 7.3.1 has Incorrect Access Control, issue 2 of 3.	5.3	More Details
CVE-2025-54983	A health check port on Zscaler Client Connector on Windows, versions 4.6 < 4.6.0.216 and 4.7 < 4.7.0.47, which under specific circumstances was not released after use, allowed traffic to potentially bypass ZCC forwarding controls.	5.2	More Details
CVE-2025-60686	A local stack-based buffer overflow vulnerability exists in the infostat.cgi and cstecgi.cgi binaries of ToToLink routers (A720R V4.1.5cu.614_B20230630, LR1200GB V9.1.0u.6619_B20230130, and NR1800X V9.1.0u.6681_B20230703). Both programs parse the contents of /proc/net/arp using sscanf() with "%s" format specifiers into fixed-size stack buffers without length validation. Specifically, one function writes user-controlled data into a single-byte buffer, and the other into adjacent small arrays without bounds checking. An attacker who controls the contents of /proc/net/arp can trigger memory corruption, leading to denial of service or potential arbitrary code execution.	5.1	More Details
CVE-2025-63408	Local Agent DVR versions thru 6.6.1.0 are vulnerable to directory traversal that allows an unauthenticated local attacker to gain access to sensitive information, cause a server-side forgery request (SSRF), or execute OS commands.	5.1	More Details
CVE-2025-60685	A stack buffer overflow exists in the ToToLink A720R Router firmware V4.1.5cu.614_B20230630 within the sysconf binary (sub_401EE0 function). The binary reads the /proc/stat file using fgets() into a local buffer and subsequently parses the line using sscanf() into a single-byte variable with the %s format specifier. Maliciously crafted /proc/stat content can overwrite adjacent stack memory, potentially allowing an attacker with filesystem write privileges to execute arbitrary code on the device.	5.1	More Details
CVE-2025-64738	External control of file name or path in Zoom Workplace for macOS before version 6.5.10 may allow an authenticated user to conduct a disclosure of information via local access.	5.0	More Details
CVE-2025-64706	Typebot is an open-source chatbot builder. In version 3.9.0 up to but excluding version 3.13.0, an Insecure Direct Object Reference (IDOR) vulnerability exists in the API token management endpoint. An authenticated attacker can delete any user's API token and retrieve its value by simply knowing the target user's ID and token ID, without requiring authorization checks. Version 3.13.0 fixes the issue.	5.0	More Details
CVE-2025-	Mattermost versions 10.11.x <= 10.11.3, 10.5.x <= 10.5.11, 10.12.x <= 10.12.0 fail to sanitize user data which allows system administrators to access password hashes and MFA secrets via the POST	4.9	More

11794	/api/v4/users/{user_id}/email/verify/member endpoint		Details
CVE-2025-12620	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to generic SQL Injection via the ‘filterbyauthor’ parameter in all versions up to, and including, 6.0.7 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-2025-61664	A vulnerability in the GRUB2 bootloader has been identified in the normal module. This flaw, a memory Use After Free issue, occurs because the normal_exit command is not properly unregistered when its related module is unloaded. An attacker can exploit this condition by invoking the command after the module has been removed, causing the system to improperly access a previously freed memory location. This leads to a system crash or possible impacts in data confidentiality and integrity.	4.9	More Details
CVE-2025-11981	The School Management System – WPSchoolPress plugin for WordPress is vulnerable to SQL Injection via the 'SCodes' parameter in all versions up to, and including, 2.2.23 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-2025-61663	A vulnerability has been identified in the GRUB2 bootloader's normal command that poses an immediate Denial of Service (DoS) risk. This flaw is a Use-after-Free issue, caused because the normal command is not properly unregistered when the module is unloaded. An attacker who can execute this command can force the system to access memory locations that are no longer valid. Successful exploitation leads directly to system instability, which can result in a complete crash and halt system availability. Impact on the data integrity and confidentiality is also not discarded.	4.9	More Details
CVE-2025-61662	A Use-After-Free vulnerability has been discovered in GRUB's gettext module. This flaw stems from a programming error where the gettext command remains registered in memory after its module is unloaded. An attacker can exploit this condition by invoking the orphaned command, causing the application to access a memory location that is no longer valid. An attacker could exploit this vulnerability to cause grub to crash, leading to a Denial of Service. Possible data integrity or confidentiality compromise is not discarded.	4.9	More Details
CVE-2025-8870	On affected platforms running Arista EOS, certain serial console input might result in an unexpected reload of the device.153	4.9	More Details
CVE-2025-54771	A use-after-free vulnerability has been identified in the GNU GRUB (Grand Unified Bootloader). The flaw occurs because the file-closing process incorrectly retains a memory pointer, leaving an invalid reference to a file system structure. An attacker could exploit this vulnerability to cause grub to crash, leading to a Denial of Service. Possible data integrity or confidentiality compromise is not discarded.	4.9	More Details
CVE-2025-54770	A vulnerability has been identified in the GRUB2 bootloader's network module that poses an immediate Denial of Service (DoS) risk. This flaw is a Use-after-Free issue, caused because the net_set_vlan command is not properly unregistered when the network module is unloaded from memory. An attacker who can execute this command can force the system to access memory locations that are no longer valid. Successful exploitation leads directly to system instability, which can result in a complete crash and halt system availability	4.9	More Details
CVE-2025-13163	EasyFlow GP developed by Digiwin has an Insufficiently Protected Credentials vulnerability, allowing privileged remote attackers to obtain plaintext database account credentials from the system frontend.	4.9	More Details
CVE-2025-13164	EasyFlow GP developed by Digiwin has an Insufficiently Protected Credentials vulnerability, allowing privileged remote attackers to obtain plaintext credentials of AD and system mail from the system frontend.	4.9	More Details
CVE-2025-12869	The a+HRD developed by aEnrich has a Stored Cross-Site Scripting vulnerability, allowing remote attackers with administrator privileges to inject persistent JavaScript codes that are executed in users' browsers upon page load.	4.8	More Details
CVE-2025-55059	CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	4.8	More Details
CVE-2025-40545	SolarWinds Observability Self-Hosted is susceptible to an open redirection vulnerability. The URL is not properly sanitized, and an attacker could manipulate the string to redirect a user to a malicious site. The attack complexity is high, and authentication is required.	4.8	More Details
CVE-2025-	Multiple CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	4.8	More

55056			Details
CVE-2025-64758	@dependencytrack/frontend is a Single Page Application (SPA) used in Dependency-Track, an open source Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain. Since version 4.12.0, Dependency-Track users with the SYSTEM_CONFIGURATION permission can configure a "welcome message", which is HTML that is to be rendered on the login page for branding purposes. When rendering the welcome message, Dependency-Track versions before 4.13.6 did not properly sanitize the HTML, allowing arbitrary JavaScript to be executed. Users with the SYSTEM_CONFIGURATION permission (i.e., administrators), can exploit this weakness to execute arbitrary JavaScript for users browsing to the login page. The issue has been fixed in version 4.13.6.	4.8	More Details
CVE-2025-30669	Improper certificate validation in certain Zoom Clients may allow an unauthenticated user to conduct a disclosure of information via adjacent access.	4.8	More Details
CVE-2025-10018	QuickCMS is vulnerable to multiple Stored XSS in language editor functionality (languages). Malicious attacker with admin privileges can inject arbitrary HTML and JS into website, which will be rendered/executed on every page. By default admin user is not able to add JavaScript into the website. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	4.8	More Details
CVE-2025-11560	The Team Members Showcase WordPress plugin before 3.5.0 does not sanitize and escape a parameter before outputting it back in the page, leading to reflected cross-site scripting, which could be used against high-privilege users such as admins.	4.8	More Details
CVE-2025-61661	A vulnerability has been identified in the GRUB (Grand Unified Bootloader) component. This flaw occurs because the bootloader mishandles string conversion when reading information from a USB device, allowing an attacker to exploit inconsistent length values. A local attacker can connect a maliciously configured USB device during the boot sequence to trigger this issue. A successful exploitation may lead GRUB to crash, leading to a Denial of Service. Data corruption may be also possible, although given the complexity of the exploit the impact is most likely limited.	4.8	More Details
CVE-2025-13275	A security vulnerability has been detected in Iqbolshoh php-business-website up to 10677743a8dfc281f85291a27cf63a0bce043c24. This affects an unknown part of the file /admin/about.php. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	4.7	More Details
CVE-2025-13185	A security flaw has been discovered in Bdtask/CodeCanyon News365 up to 7.0.3. This affects an unknown function of the file /admin/dashboard/profile. The manipulation of the argument profile_image/banner_image results in unrestricted upload. 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.	4.7	More Details
CVE-2025-20355	A vulnerability in the web-based management interface of Cisco Catalyst Center Virtual Appliance could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by intercepting and modifying an HTTP request from a user. A successful exploit could allow the attacker to redirect the user to a malicious web page.	4.7	More Details
CVE-2025-13302	A vulnerability was identified in code-projects Courier Management System 1.0. This affects an unknown part of the file /add-new-officer.php. Such manipulation of the argument ManagerName leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2025-13076	A flaw has been found in code-projects Responsive Hotel Site 1.0. The affected element is an unknown function of the file /admin/usersetting.php. Executing manipulation of the argument usname can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2025-13075	A vulnerability was detected in code-projects Responsive Hotel Site 1.0. Impacted is an unknown function of the file /admin/usersettingdel.php. Performing manipulation of the argument eid results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	4.7	More Details
CVE-2025-13210	A security vulnerability has been detected in itsourcecode Inventory Management System 1.0. This impacts an unknown function of the file /admin/products/index.php?view=add. Such manipulation of the argument PROMODEL leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-13198	A vulnerability has been found in DouPHP up to 1.8 Release 20251022. This impacts an unknown function of the file upload/include/file.class.php. The manipulation of the argument File leads to unrestricted upload. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	4.7	More Details

CVE-2024-46335	PHPGurukul Complaint Management System 2.0 is vulnerble to Cross Site Scripting (XSS) via the fromdate and todate parameters in between-date-userreport.php.	4.6	More Details
CVE-2025-64746	Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 11.13.0, Directus does not properly clean up field-level permissions when a field is deleted. When a field is removed from a collection, its reference in the permissions table remains intact. This stale reference creates a security gap: if another field is later created using the same name, it inherits the outdated permission entry. This behavior can unintentionally grant roles access to data they should not be able to read or modify. The issue is particularly risky in multi-tenant or production environments, where administrators may reuse field names, assuming old permissions have been fully cleared. Version 11.13.0 fixes the issue.	4.6	More Details
CVE-2025-64482	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Tuleap Community Edition prior to version 16.13.99.1762267347 and Tuleap Enterprise Edition prior to versions 17.01-, 16.13-6, and 16.12-9 don't have cross-site request forgery protections in the file release system. An attacker could use this vulnerability to trick victims into changing the commit rules or immutable tags of a SVN repo. Tuleap Community Edition 16.13.99.1762267347, Tuleap Enterprise Edition 17.0-1, Tuleap Enterprise Edition 16.13-6, and Tuleap Enterprise Edition 16.12-9 fix the issue.	4.6	More Details
CVE-2025-64117	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Tuleap Community Edition prior to version 16.13.99.1761813675 and Tuleap Enterprise Edition prior to versions 16.13-5 and 16.12-8 don't have cross-site request forgery protection in the management of SVN commit rules and immutable tags. An attacker could use this vulnerability to trick victims into changing the commit rules or immutable tags of a SVN repo. Tuleap Community Edition 16.13.99.1761813675, Tuleap Enterprise Edition 16.13-5, and Tuleap Enterprise Edition 16.12-8 contain a fix for the issue.	4.6	More Details
CVE-2025-55058	CWE-20 Improper Input Validation	4.5	More Details
CVE-2025-55057	Multiple CWE-352 Cross-Site Request Forgery (CSRF)	4.5	More Details
CVE-2025-12018	The MembershipWorks – Membership, Events & Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 6.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-64517	sudo-rs is a memory safe implementation of sudo and su written in Rust. With `Defaults targetpw` (or `Defaults rootpw`) enabled, the password of the target account (or root account) instead of the invoking user is used for authentication. sudo-rs starting in version 0.2.5 and prior to version 0.2.10 incorrectly recorded the invoking user’s UID instead of the authenticated-as user's UID in the authentication timestamp. Any later `sudo` invocation on the same terminal while the timestamp was still valid would use that timestamp, potentially bypassing new authentication even if the policy would have required it. A highly-privileged user (able to run commands as other users, or as root, through sudo) who knows one password of an account they are allowed to run commands as, would be able to run commands as any other account the policy permits them to run commands for, even if they don't know the password for those accounts. A common instance of this would be that a user can still use their own password to run commands as root (the default behaviour of `sudo`), effectively negating the intended behaviour of the `targetpw` or `rootpw` options. Version 0.2.10 contains a patch for the issue. Versions prior to 0.2.5 are not affected, since they do not offer `Defaults targetpw` or `Defaults rootpw`.	4.4	More Details
CVE-2025-64267	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in WPSwings WooCommerce Ultimate Points And Rewards woocommerce-ultimate-points-and-rewards allows Retrieve Embedded Sensitive Data.This issue affects WooCommerce Ultimate Points And Rewards: from n/a through <= 2.10.2.	4.3	More Details
CVE-2025-12481	The WP Duplicate Page plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.7. This is due to the plugin not properly verifying that a user is authorized to perform an action in the 'saveSettings' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to modify plugin settings that control role capabilities, and subsequently exploit the misconfigured capabilities to duplicate and view password-protected posts containing sensitive information.	4.3	More Details
CVE-2025-12639	The wModes – Catalog Mode, Product Pricing, Enquiry Forms & Promotions plugin for WordPress is vulnerable to authorization bypass in versions up to, and including, 1.2.2. This is due to the plugin not properly verifying that a user is authorized to access sensitive information via the AJAX endpoint. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract sensitive information including user emails, usernames, roles, capabilities, and WooCommerce data such as products and payment methods.	4.3	More Details

CVE-2025-64265	Missing Authorization vulnerability in N-Media Frontend File Manager nmedia-user-file-uploader allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Frontend File Manager: from n/a through <= 23.2.	4.3	More Details
CVE-2025-64406	An out-of-bounds Write vulnerability in Apache OpenOffice could allow an attacker to craft a document that would crash the program, or otherwise corrupt other memory areas. This issue affects Apache OpenOffice: through 4.1.15. Users are recommended to upgrade to version 4.1.16, which fixes the issue.	4.3	More Details
CVE-2025-64269	Missing Authorization vulnerability in EDGARROJAS WooCommerce PDF Invoice Builder woo-pdf-invoice-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce PDF Invoice Builder: from n/a through <= 1.2.150.	4.3	More Details
CVE-2025-64274	Missing Authorization vulnerability in wpkoithemes WPKoi Templates for Elementor wpkoi-templates-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPKoi Templates for Elementor: from n/a through <= 3.4.4.	4.3	More Details
CVE-2025-27368	IBM OpenPages 9.0 and 9.1 is vulnerable to information disclosure of sensitive information due to a weaker than expected security for certain REST end points used by the user interface of OpenPages. An authenticated user is able to obtain certain information about system metadata for areas beyond what the user is intended to view.	4.3	More Details
CVE-2025-9625	The Coil Web Monetization plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.2. This is due to missing or incorrect nonce validation on the coil-get-css-selector parameter handling in the maybe_restrict_content function. This makes it possible for unauthenticated attackers to trigger CSS selector detection functionality 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-2025-12015	The Convert WebP & AVIF | Quicq | Best image optimizer and compression plugin | Improve your Google Pagespeed plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_wpqai_disconnect_quicq_afosto' AJAX endpoint in all versions up to, and including, 2.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect Afosto	4.3	More Details
CVE-2025-12961	The Download Panel plugin for WordPress is vulnerable to unauthorized settings modification due to a missing capability check on the 'wp_ajax_save_settings' AJAX action in all versions up to, and including, 1.3.3. This is due to the absence of any capability verification in the `dlpn_save_settings()` function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to arbitrarily modify plugin settings including display text, download links, button colors, and other visual customizations.	4.3	More Details
CVE-2025-12827	The Top Friends plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.3. This is due to missing nonce validation on the top_friends_options_subpanel() function. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12372	The Permalinks Cascade plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.2. This is due to the plugin not properly verifying that a user is authorized to perform an action in the handleTPCAdminAjaxRequest function. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform unauthorized administrative actions such as enabling or disabling automatic pinging settings and modifying page exclusion settings.	4.3	More Details
CVE-2025-12173	The WP Admin Microblog plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.1. This is due to missing or incorrect nonce validation on the 'wp-admin-microblog' page. This makes it possible for unauthenticated attackers to send messages on behalf of an administrator 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-2025-10158	A malicious client acting as the receiver of an rsync file transfer can trigger an out of bounds read of a heap based buffer, via a negative array index. The malicious rsync client requires at least read access to the remote rsync module in order to trigger the issue.	4.3	More Details
CVE-2025-12366	The Page Builder: Pagelayer – Drag and Drop website builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.0.5 via the pagelayer_replace_page function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to replace media files belonging to other users, including administrators.	4.3	More Details
CVE-2025-64705	Frappe Learning is a learning system that helps users structure their content. Starting in version 2.0.0 and prior to version 2.41.0, users were able to access the submissions made by other students The issue has been fixed in version 2.41.0 by ensuring proper roles and redirecting if accessed via direct URL.	4.3	More Details
CVE-2025-36299	IBM Planning Analytics Local 2.1.0 through 2.1.14 stores sensitive information in source code could be used in further attacks against the system.	4.3	More Details

CVE-2025-64379	Missing Authorization vulnerability in Pluggabl Booster for WooCommerce woocommerce-jetpack allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booster for WooCommerce: from n/a through <= 7.4.0.	4.3	More Details
CVE-2025-54971	An exposure of sensitive information to an unauthorized actor vulnerability in Fortinet FortiADC 7.4.0, FortiADC 7.2 all versions, FortiADC 7.1 all versions, FortiADC 7.0 all versions, FortiADC 6.2 all versions may allow an admin with read-only permission to get the external resources password via the logs of the product	4.3	More Details
CVE-2025-53360	pluginsGLPI's Database Inventory Plugin "manages" the Teclib' inventory agents in order to perform an inventory of the databases present on the workstation. In versions prior to 1.0.3, any authenticated user could send requests to agents. This issue has been patched in version 1.0.3.	4.3	More Details
CVE-2025-13082	User Interface (UI) Misrepresentation of Critical Information vulnerability in Drupal Drupal core allows Content Spoofing.This issue affects Drupal core: from 8.0.0 before 10.4.9, from 10.5.0 before 10.5.6, from 11.0.0 before 11.1.9, from 11.2.0 before 11.2.8.	4.3	More Details
CVE-2025-54972	An improper neutralization of crlf sequences ('crlf injection') in Fortinet FortiMail 7.6.0 through 7.6.3, FortiMail 7.4.0 through 7.4.5, FortiMail 7.2 all versions, FortiMail 7.0 all versions may allow an attacker to inject headers in the response via convincing a user to click on a specifically crafted link	4.3	More Details
CVE-2025-37734	Origin Validation Error in Kibana can lead to Server-Side Request Forgery via a forged Origin HTTP header processed by the Observability AI Assistant.	4.3	More Details
CVE-2025-64382	Missing Authorization vulnerability in WebToffee Order Export & Order Import for WooCommerce order-import-export-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Order Export & Order Import for WooCommerce: from n/a through <= 2.6.7.	4.3	More Details
CVE-2025-12182	The Qi Blocks plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the `resize_image_callback()` function in all versions up to, and including, 1.4.3. This is due to the plugin not properly verifying that a user has permission to resize a specific attachment. This makes it possible for authenticated attackers, with Contributor-level access and above, to resize arbitrary media library images belonging to other users, which can result in unintended file writes, disk consumption, and server resource abuse through processing of large images.	4.3	More Details
CVE-2024-11919	Inappropriate implementation in Intents in Google Chrome on Android prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2025-11865	An issue has been discovered in GitLab EE affecting all versions from 18.1 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2 that, under certain circumstances, could have allowed an attacker to remove Duo flows of another user.	4.3	More Details
CVE-2025-20346	A vulnerability in Cisco Catalyst Center could allow an authenticated, remote attacker to execute operations that should require Administrator privileges. The attacker would need valid read-only user credentials. This vulnerability is due to improper role-based access control (RBAC). An attacker could exploit this vulnerability by logging in to an affected system and modifying certain policy configurations. A successful exploit could allow the attacker to modify policy configurations that are reserved for the Administrator role. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Observer.	4.3	More Details
CVE-2025-54561	An Incorrect Access Control vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows remote access to content despite lack of the correct permission through a Broken Authorization Schema.	4.3	More Details
CVE-2025-54562	A vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows Technical Information to be Disclosed through stack trace.	4.3	More Details
CVE-2025-64749	Directus is a real-time API and App dashboard for managing SQL database content. An observable difference in error messaging was found in the Directus REST API in versions of Directus prior to version 11.13.0. The `/items/{collection}` API returns different error messages for two cases: when a user tries to access an existing collection which they are not authorized to access, and when user tries to access a non-existing collection. The two differing error messages leak the existence of collections to users which are not authorized to access these collections. Version 11.13.0 fixes the issue.	4.3	More Details
CVE-2025-13177	A vulnerability was detected in Bdtask/CodeCanyon SalesERP up to 20250728. This affects an unknown part. The manipulation results in cross-site request forgery. 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-	A vulnerability has been found in Bdtask/CodeCanyon Wholesale Inventory Control and Inventory Management System up to 20250320. This issue affects some unknown processing. Such manipulation leads to cross-site request forgery. The attack may be performed from remote. The exploit has been disclosed to	4.3	More

13179	the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2025-12847	The All in One SEO – Powerful SEO Plugin to Boost SEO Rankings & Increase Traffic plugin for WordPress is vulnerable to unauthorized arbitrary media attachment deletion due to a missing authorization check in all versions up to, and including, 4.8.9. This is due to the REST API endpoint `/wp-json/aioseo/v1/ai/image-generator` only verifying that users have the `edit_posts` capability (Contributors and above) without checking if they own or have permission to delete the specific media attachments. This makes it possible for authenticated attackers, with Contributor-level access and above, to permanently delete arbitrary media attachments by ID via the REST API, granted they can determine valid attachment IDs.	4.3	More Details
CVE-2025-63744	A NULL pointer dereference vulnerability was discovered in radare2 6.0.5 and earlier within the load() function of bin_dyldcache.c. Processing a crafted file can cause a segmentation fault and crash the program.	4.3	More Details
CVE-2025-12494	The Image Gallery – Photo Grid & Video Gallery plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the ajax_import_file function in all versions up to, and including, 2.12.28. This makes it possible for authenticated attackers, with author-level access and above, to move arbitrary image files on the server.	4.3	More Details
CVE-2025-12732	The WP Import – Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to unauthorized access of sensitive information due to a missing authorization check on the showsetting() function in all versions up to, and including, 7.33. This makes it possible for authenticated attackers, with Author-level access or higher, to extract sensitive information including OpenAI API keys configured through the plugin's admin interface.	4.3	More Details
CVE-2025-12087	The Wishlist and Save for later for Woocommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.22 via the 'awwlm_remove_added_wishlist_page' AJAX action due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete wishlist items from other user's wishlists.	4.3	More Details
CVE-2025-12833	The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.8.139 via the 'post_attachment_upload' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with author-level access and above, to attach arbitrary image files to arbitrary places.	4.3	More Details
CVE-2025-12901	The Asgaros Forum plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.1. This is due to missing nonce validation on the set_subscription_level() function. This makes it possible for unauthenticated attackers to modify the subscription settings of authenticated users via a forged request granted they can trick a logged-in user into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-2615	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.7 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2, that could have allowed a blocked user to access sensitive information by establishing GraphQL subscriptions through WebSocket connections.	4.3	More Details
CVE-2024-11920	Inappropriate implementation in Dawn in Google Chrome on Mac prior to 130.0.6723.92 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2025-7000	An issue has been discovered in GitLab CE/EE affecting all versions from 17.6 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2, that, under specific conditions, could have allowed unauthorized users to view confidential branch names by accessing project issues with related merge requests.	4.3	More Details
CVE-2025-13239	A security vulnerability has been detected in Bdtask/CodeCanyon Isshue Multi Store eCommerce Shopping Cart Solution 5. Affected by this issue is some unknown functionality of the file /submit_checkout. Such manipulation of the argument order_total_amount/cart_total_amount leads to enforcement of behavioral workflow. 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.	4.3	More Details
CVE-2025-11776	Mattermost versions <11 fail to properly restrict access to archived channel search API which allows guest users to discover archived public channels via the `/api/v4/teams/{team_id}/channels/search_archived` endpoint	4.3	More Details
CVE-2025-13115	A security flaw has been discovered in macrozheng mall-swarm and mall up to 1.0.3. This impacts the function detail of the file /order/detail/ of the component Order Details Handler. Performing manipulation of the argument orderId results in improper authorization. It is possible to initiate the attack 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.	4.3	More Details
CVE-2025-	Out of bounds read in V8 in Google Chrome prior to 133.0.6943.141 allowed a remote attacker to potentially	4.3	More

9479	exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)		Details
CVE-2025-13107	Inappropriate implementation in Compositing in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2025-13244	A vulnerability was determined in code-projects Student Information System 2.0. The affected element is an unknown function of the file /register.php. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2025-13119	A flaw has been found in Fabian Ros/SourceCodester Simple E-Banking System 1.0. This affects an unknown part. This manipulation causes cross-site request forgery. The attack may be initiated remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-62482	Cross-site scripting in Zoom Workplace for Windows before version 6.5.10 may allow an unauthenticated user to impact integrity via network access.	4.3	More Details
CVE-2025-64739	External control of file name or path in certain Zoom Clients may allow an unauthenticated user to conduct a disclosure of information via network access.	4.3	More Details
CVE-2025-13102	Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 134.0.6998.35 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2025-12113	The Alt Text Generator AI – Auto Generate & Bulk Update Alt Texts For Images plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the atgai_delete_api_key() function in all versions up to, and including, 1.8.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the API key connected to the site.	4.3	More Details
CVE-2024-7021	Inappropriate implementation in Autofill in Google Chrome on Windows prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-13178	Inappropriate implementation in Fullscreen in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2025-64515	Open Forms allows users create and publish smart forms. Prior to versions 3.2.7 and 3.3.3, forms where the prefill data fields are dynamically set to readonly/disabled can be modified by malicious users deliberately trying to modify data they're not supposed to. For regular users, the form fields are marked as readonly and cannot be modified through the user interface. This issue has been patched in versions 3.2.7 and 3.3.3.	4.3	More Details
CVE-2025-61713	A Cleartext Storage of Sensitive Information in Memory vulnerability [CWE-316] in Fortinet FortiPAM 1.6.0, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions may allow an authenticated attacker with read-write admin privileges to the CLI to obtain other administrators' credentials via diagnose commands.	4.2	More Details
CVE-2025-54340	A vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2. There is a Broken or Risky Cryptographic Algorithm.	4.1	More Details
CVE-2025-63927	A heap-use-after-free vulnerability exists in airpig2011 IEC104 thru Commit be6d841 (2019-07-08). During multi-threaded client execution, the function Iec10x_Scheduled can access memory that has already been freed, potentially causing program crashes or undefined behavior. This may be exploited to trigger a denial-of-service or memory corruption.	4.0	More Details
CVE-2025-43205	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in watchOS 11.4, tvOS 18.4, visionOS 2.4, iOS 18.4 and iPadOS 18.4. An app may be able to bypass ASLR.	4.0	More Details
CVE-2025-64503	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. In cups-filters prior to 1.28.18, by crafting a PDF file with a large `MediaBox` value, an attacker can cause CUPS-Filter 1.x's `pdftoraster` tool to write beyond the bounds of an array. First, a PDF with a large `MediaBox` width value causes `header.cupsWidth` to become large. Next, the calculation of `bytesPerLine = (header.cupsBitsPerPixel * header.cupsWidth + 7) / 8` overflows, resulting in a small value. Then, `lineBuf` is allocated with the small `bytesPerLine` size. Finally, `convertLineChunked` calls `writePixel8`, which attempts to write to `lineBuf` outside of its buffer size (out of bounds write). In libcupsfilters, the maintainers found the same `bytesPerLine` multiplication without overflow check, but the provided test case does not cause an overflow there, because the values are different. Commit 50d94ca0f2fa6177613c97c59791bde568631865 contains a patch, which is incorporated into cups-filters version 1.28.18.	4.0	More Details

CVE-2025-64711	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. Starting in version 1.7.7 and prior to version 2.0.3, dragging a file whose filename contains HTML is reflected verbatim into the page via the drag-and-drop helper, so any user who drops a crafted file on PrivateBin will execute arbitrary JavaScript within their own session (self-XSS). This allows an attacker who can entice a victim to drag or otherwise attach such a file to exfiltrate plaintext, encryption keys, or stored pastes before they are encrypted or sent. Certain conditions must exist for the vulnerability to be exploitable. Only macOS or Linux users are affected, due to the way the `>` character is treated in a file name on Windows. The PrivateBin instance needs to have file upload enabled. An attacker needs to have access to the local file system or somehow convince the user to create (or download) a malicious file (name). An attacker needs to convince the user to attach that malicious file to PrivateBin. Any Mac / Linux user who can be tricked into dragging a maliciously named file into the editor is impacted; code runs in the origin of the PrivateBin instance they are using. Attackers can steal plaintext, passphrases, or manipulate the UI before data is encrypted, defeating the zero-knowledge guarantees for that victim session, assuming counter-measures like Content-Security-Policy (CSP) have been disabled. If CSP is not disabled, HTML injection attacks may be possible - like redirecting to a foreign website, phishing etc. As the whole exploit needs to be included in the file name of the attached file and only affects the local session of the user (aka it is neither persistent nor remotely executable) and that user needs to interact and actively attach that file to the paste, the impact is considered to be practically low. Version 2.0.3 patches the issue.	3.9	More Details
CVE-2025-54560	A Server-side Request Forgery vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows Probing of internal infrastructure.	3.8	More Details
CVE-2025-64170	sudo-rs is a memory safe implementation of sudo and su written in Rust. Starting in version 0.2.7 and prior to version 0.2.10, if a user begins entering a password but does not press return for an extended period, a password timeout may occur. When this happens, the keystrokes that were entered are echoed back to the console. This could reveal partial password information, possibly exposing history files when not carefully handled by the user and on screen, usable for Social Engineering or Pass-By attacks. Version 0.2.10 fixes the issue.	3.8	More Details
CVE-2025-54559	An issue was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows remote Path Traversal for loading arbitrary external content.	3.7	More Details
CVE-2025-65014	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Prior to version 25.11.0, a weak password policy vulnerability was identified in the user management functionality of the LibreNMS application. This vulnerability allows administrators to create accounts with extremely weak and predictable passwords, such as 12345678. This exposes the platform to brute-force and credential stuffing attacks. This issue has been patched in version 25.11.0.	3.7	More Details
CVE-2025-13083	Use of Web Browser Cache Containing Sensitive Information vulnerability in Drupal Drupal core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Drupal core: from 8.0.0 before 10.4.9, from 10.5.0 before 10.5.6, from 11.0.0 before 11.1.9, from 11.2.0 before 11.2.8.	3.7	More Details
CVE-2025-57812	CUPS is a standards-based, open-source printing system, and `libcupsfilters` contains the code of the filters of the former `cups-filters` package as library functions to be used for the data format conversion tasks needed in Printer Applications. In CUPS-Filters versions up to and including 1.28.17 and libscupsfilters versions 2.0.0 through 2.1.1, CUPS-Filters's `imagetoraster` filter has an out of bounds read/write vulnerability in the processing of TIFF image files. While the pixel buffer is allocated with the number of pixels times a pre-calculated bytes-per-pixel value, the function which processes these pixels is called with a size of the number of pixels times 3. When suitable inputs are passed, the bytes-per-pixel value can be set to 1 and bytes outside of the buffer bounds get processed. In order to trigger the bug, an attacker must issue a print job with a crafted TIFF file, and pass appropriate print job options to control the bytes-per-pixel value of the output format. They must choose a printer configuration under which the `imagetoraster` filter or its C-function equivalent `cfFilterImageToRaster()` gets invoked. The vulnerability exists in both CUPS-Filters 1.x and the successor library libcupsfilters (CUPS-Filters 2.x). In CUPS-Filters 2.x, the vulnerable function is `_cfImageReadTIFF() in libcupsfilters`. When this function is invoked as part of `cfFilterImageToRaster()`, the caller passes a look-up-table during whose processing the out of bounds memory access happens. In CUPS-Filters 1.x, the equivalent functions are all found in the cups-filters repository, which is not split into subprojects yet, and the vulnerable code is in `_cupsImageReadTIFF()`, which is called through `cupsImageOpen()` from the `imagetoraster` tool. A patch is available in commit b69dfacec7f176281782e2f7ac44f04bf9633cfa.	3.7	More Details
CVE-2025-13178	A flaw has been found in Bdtask/CodeCanyon SalesERP up to 20250728. This vulnerability affects unknown code of the file /edit_profile of the component User Profile Handler. This manipulation of the argument first_name/last_name causes basic cross site scripting. 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.	3.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal		More

2025-12761	Simple multi step form allows Cross-Site Scripting (XSS).This issue affects Simple multi step form: from 0.0.0 before 2.0.0.	3.5	Details
CVE-2025-6945	GitLab has remediated an issue in GitLab EE affecting all versions from 17.8 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2 that could have allowed an authenticated attacker to leak sensitive information from confidential issues by injecting hidden prompts into merge request comments.	3.5	More Details
CVE-2025-13349	A vulnerability has been found in SourceCodester Student Grades Management System 1.0. This issue affects some unknown processing of the file /grades.php of the component Add New Grade Page. The manipulation of the argument Remarks leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-13182	A vulnerability was identified in pojoin h3blog 1.0. The impacted element is an unknown function of the file /admin/cms/category/addtitle. The manipulation of the argument Title leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2025-63292	Freebox v5 HD (firmware = 1.7.20), Freebox v5 Crystal (firmware = 1.7.20), Freebox v6 Révolution r1–r3 (firmware = 4.7.x), Freebox Mini 4K (firmware = 4.7.x), and Freebox One (firmware = 4.7.x) were discovered to expose subscribers' IMSI identifiers in plaintext during the initial phase of EAP-SIM authentication over the `FreeWifi_secure` network. During the EAP-Response/Identity exchange, the subscriber's full Network Access Identifier (NAI), which embeds the raw IMSI, is transmitted without encryption, tunneling, or pseudonymization. An attacker located within Wi-Fi range (~100 meters) can passively capture these frames without requiring user interaction or elevated privileges. The disclosed IMSI enables device tracking, subscriber correlation, and long-term monitoring of user presence near any broadcasting Freebox device. The vendor acknowledged the vulnerability, and the `FreeWifi_secure` service is planned for full deactivation by 1 October 2025.	3.5	More Details
CVE-2025-12983	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.9 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2 that could have allowed an authenticated attacker to cause a denial of service condition by submitting specially crafted markdown content with nested formatting patterns.	3.5	More Details
CVE-2025-64744	OpenObserve is a cloud-native observability platform. In versions up to and including 0.16.1, when creating or renaming an organization with HTML in the name, the markup is rendered inside the invitation email. This indicates that user-controlled input is inserted into the email template without proper HTML escaping. As of time of publication, no patched versions are available.	3.5	More Details
CVE-2025-13058	A security flaw has been discovered in soerennb eXtplorer up to 2.1.15. The affected element is an unknown function of the component Filename Handler. The manipulation results in cross site scripting. The attack may be launched remotely. The patch is identified as 002def70b985f7012586df2c44368845bf405ab3. Applying a patch is advised to resolve this issue.	3.5	More Details
CVE-2025-13181	A vulnerability was determined in pojoin h3blog 1.0. The affected element is an unknown function of the file /admin/cms/material/add. Executing manipulation of the argument Name can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	3.5	More Details
CVE-2025-13343	A security flaw has been discovered in SourceCodester Interview Management System 1.0. Affected is an unknown function of the file /editQuestion.php. The manipulation of the argument Question results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	3.5	More Details
CVE-2025-13232	A flaw has been found in projectsend up to r1720. Impacted is an unknown function of the component File Editor/Custom Download Aliases. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. Upgrading to version r1945 is recommended to address this issue. Patch name: 334da1ea39cb12f6b6e98dd2f80bb033e0c7b845. It is advisable to upgrade the affected component.	3.5	More Details
CVE-2025-13180	A vulnerability was found in Bdtask/CodeCanyon Wholesale Inventory Control and Inventory Management System up to 20250320. Impacted is an unknown function of the file /edit_profile. Performing manipulation of the argument first_name/last_name results in basic cross site scripting. 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.	3.5	More Details
CVE-2025-52639	HCL Connections is vulnerable to a sensitive information disclosure vulnerability which could allow a user to obtain sensitive information they are not entitled to, caused by improper rendering of application data.	3.5	More Details
CVE-2025-20379	In Splunk Enterprise versions below 10.0.1, 9.4.5, 9.3.7, and 9.2.9 and Splunk Cloud Platform versions below 9.3.2411.116, 9.3.2408.124, 10.0.2503.5 and 10.1.2507.1, a low-privileged user that does not hold the “admin“ or “power“ Splunk roles could run a saved search with a risky command using the permissions of a higher-privileged user to bypass the SPL safeguards for risky commands. They could bypass these safeguards on the “/services/streams/search“ endpoint through its “q“ parameter by circumventing endpoint restrictions using character encoding in the REST path. The vulnerability requires the attacker to phish the victim by	3.5	More Details

	tricking them into initiating a request within their browser. The authenticated user should not be able to exploit the vulnerability at will.		
CVE-2025-13245	A vulnerability was identified in code-projects Student Information System 2.0. The impacted element is an unknown function of the file /editprofile.php. Such manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2025-13202	A security flaw has been discovered in code-projects Simple Cafe Ordering System 1.0. This affects an unknown part of the file /add_to_cart. Performing manipulation of the argument product_name results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	3.5	More Details
CVE-2025-54342	A vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2. There is Exposure of Sensitive Information because of Incompatible Policies.	3.3	More Details
CVE-2025-63396	An issue was discovered in PyTorch v2.5 and v2.7.1. Omission of profiler.stop() can cause torch.profiler.profile (PythonTracer) to crash or hang during finalization, leading to a Denial of Service (DoS).	3.3	More Details
CVE-2025-46370	Dell Alienware Command Center 6.x (AWCC), versions prior to 6.10.15.0, contain a Process Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information Disclosure.	3.3	More Details
CVE-2025-12792	The Mac App Store distribution of the Canva for Mac desktop app before 1.117.1 was built without Hardened Runtime. A local threat actor with unprivileged access could execute arbitrary code that inherits the TCC (Transparency, Consent, and Control) permissions assigned to Canva.	3.2	More Details
CVE-2025-65083	GoSign Desktop through 2.4.1 disables TLS certificate validation when configured to use a proxy server. This can be problematic if the GoSign Desktop user selects an arbitrary proxy server without consideration of whether outbound HTTPS connections from the proxy server to Internet servers succeed even for untrusted or invalid server certificates. In this scenario (which is outside of the product's design objectives), integrity protection could be bypassed. In typical cases of a proxy server for outbound HTTPS traffic from an enterprise, those connections would not succeed. (Admittedly, the usual expectation is that a client application is configured to trust an enterprise CA and does not set SSL_VERIFY_NONE.) Also, it is of course unsafe to place ~/.gosign in the home directory of an untrusted user and then have other users execute downloaded files.	3.2	More Details
CVE-2025-11777	Mattermost versions 10.11.x <= 10.11.3, 10.5.x <= 10.5.11 fail to properly validate team membership permissions in the Add Channel Member API which allows users from one team to access user metadata and channel membership information from other teams via the API endpoint	3.1	More Details
CVE-2025-11990	GitLab has remediated an issue in GitLab EE affecting all versions from 18.4 before 18.4.4, and 18.5 before 18.5.2 that could have allowed an authenticated user to gain CSRF tokens by exploiting improper input validation in repository references combined with redirect handling weaknesses.	3.1	More Details
CVE-2025-7736	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.9 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2 that could have allowed an authenticated attacker to bypass access control restrictions and view GitLab Pages content intended only for project members by authenticating through OAuth providers.	3.1	More Details
CVE-2025-20378	In Splunk Enterprise versions below 10.0.1, 9.4.5, 9.3.7, 9.2.9, and Splunk Cloud Platform versions below 10.0.2503.5, 9.3.2411.111, and 9.3.2408.121, an unauthenticated attacker could craft a malicious URL using the `return_to` parameter of the Splunk Web login endpoint. When an authenticated user visits the malicious URL, it could cause an unvalidated redirect to an external malicious site. To be successful, the attacker has to trick the victim into initiating a request from their browser. The unauthenticated attacker should not be able to exploit the vulnerability at will.	3.1	More Details
CVE-2025-41436	Mattermost versions <11.0 fail to properly enforce the "Allow users to view archived channels" setting which allows regular users to access archived channel content and files via the "Open in Channel" functionality from followed threads	3.1	More Details
CVE-2025-12817	Missing authorization in PostgreSQL CREATE STATISTICS command allows a table owner to achieve denial of service against other CREATE STATISTICS users by creating in any schema. A later CREATE STATISTICS for the same name, from a user having the CREATE privilege, would then fail. Versions before PostgreSQL 18.1, 17.7, 16.11, 15.15, 14.20, and 13.23 are affected.	3.1	More Details
CVE-2025-55074	Mattermost versions 10.11.x <= 10.11.3, 10.5.x <= 10.5.11 fail to enforce access permissions on the Agents plugin which allows other users to determine when users had read channels via channel member objects	3.0	More Details
	Astro is a web framework. Starting in version 5.2.0 and prior to version 5.15.6, a Reflected Cross-Site Scripting (XSS) vulnerability exists in Astro's development server error pages when the `trailingSlash`		

CVE-2025-64745	configuration option is used. An attacker can inject arbitrary JavaScript code that executes in the victim's browser context by crafting a malicious URL. While this vulnerability only affects the development server and not production builds, it could be exploited to compromise developer environments through social engineering or malicious links. Version 5.15.6 fixes the issue.	2.7	More Details
CVE-2025-64734	Missing Release of Resource after Effective Lifetime (CWE-772) in the T21 Reader allows an attacker with physical access to the Reader to perform a denial-of-service attack against that specific reader, preventing cardholders from badging for entry. This issue affects Command Centre Server: 9.30 prior to vCR9.30.251028a (distributed in 9.30.2881 (MR3)), 9.20 prior to vCR9.20.251028a (distributed in 9.20.3265 (MR5)), 9.10 prior to vCR9.10.251028a (distributed in 9.10.4135 (MR8)), all versions of 9.00 and prior.	2.4	More Details
CVE-2025-13186	A weakness has been identified in Bdtask/CodeCanyon Isshue Multi Store eCommerce Shopping Cart Solution up to 4.0. This impacts an unknown function of the file /dashboard/Ccustomer/manage_customer. This manipulation of the argument Search causes cross site scripting. 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.	2.4	More Details
CVE-2025-54821	An Improper Privilege Management vulnerability [CWE-269] in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.6.0, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions may allow an authenticated administrator to bypass the trusted host policy via crafted CLI command.	1.9	More Details
CVE-2025-64345	Wasmtime is a runtime for WebAssembly. Prior to version 38.0.4, 37.0.3, 36.0.3, and 24.0.5, Wasmtime's Rust embedder API contains an unsound interaction where a WebAssembly shared linear memory could be viewed as a type which provides safe access to the host (Rust) to the contents of the linear memory. This is not sound for shared linear memories, which could be modified in parallel, and this could lead to a data race in the host. Patch releases have been issued for all supported versions of Wasmtime, notably: 24.0.5, 36.0.3, 37.0.3, and 38.0.4. These releases reject creation of shared memories via `Memory::new` and shared memories are now excluded from core dumps. As a workaround, eembeddings affected by this issue should use `SharedMemory::new` instead of `Memory::new` to create shared memories. Affected embeddings should also disable core dumps if they are unable to upgrade. Note that core dumps are disabled by default but the wasm threads proposal (and shared memory) is enabled by default.	1.8	More Details
CVE-2025-59111	Windu CMS is vulnerable to Broken Access Control in user editing functionality. Malicious attacker can send a GET request which allows privileged users to delete Super Admins which is not possible with GUI. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-40148	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add NULL pointer checks in dc_stream cursor attribute functions The function dc_stream_set_cursor_attributes() currently dereferences the `stream` pointer and nested members `stream->ctx->dc->current_state` without checking for NULL. All callers of these functions, such as in `dcn30_apply_idle_power_optimizations()` and `amdgpu_dm_plane_handle_cursor_update()`, already perform NULL checks before calling these functions. Fixes below: drivers/gpu/drm/amd/amdgpu/../display/dc/core/dc_stream.c:336 dc_stream_program_cursor_attributes() error: we previously assumed 'stream' could be null (see line 334) drivers/gpu/drm/amd/amdgpu/../display/dc/core/dc_stream.c 327 bool dc_stream_program_cursor_attributes(328 struct dc_stream_state *stream, 329 const struct dc_cursor_attributes *attributes) 330 { 331 struct dc *dc; 332 bool reset_idle_optimizations = false; 333 334 dc = stream ? stream->ctx->dc : NULL; ^^^^^^ The old code assumed stream could be NULL. 335 --> 336 if (dc_stream_set_cursor_attributes(stream, attributes)) { ^^^^^^ The refactor added an unchecked dereference. drivers/gpu/drm/amd/amdgpu/../display/dc/core/dc_stream.c 313 bool dc_stream_set_cursor_attributes(314 struct dc_stream_state *stream, 315 const struct dc_cursor_attributes *attributes) 316 { 317 bool result = false; 318 319 if (dc_stream_check_cursor_attributes(stream, stream->ctx->dc->current_state, attributes)) { ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ Here. This function used to check for if stream as NULL and return false at the start. Probably we should add that back.	N/A	More Details
CVE-2025-40149	In the Linux kernel, the following vulnerability has been resolved: tls: Use __sk_dst_get() and dst_dev_rcu() in get_netdev_for_sock(). get_netdev_for_sock() is called during setsockopt(), so not under RCU. Using sk_dst_get(sk)->dev could trigger UAF. Let's use __sk_dst_get() and dst_dev_rcu(). Note that the only ->ndo_sk_get_lower_dev() user is bond_sk_get_lower_dev(), which uses RCU.	N/A	More Details
CVE-2025-59110	Windu CMS is vulnerable to Cross-Site Request Forgery in user editing functionality. Implemented CSRF protection mechanism can be bypassed by using CSRF token of other user. It is worth noting that the registration is open and anyone can create an account. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
	Windu CMS is vulnerable to Cross-Site Request Forgery in file uploading functionality. Malicious attacker can		

CVE-2025-59114	craft special website, which when visited by the victim, will automatically send malicious file to the server. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-59112	Windu CMS is vulnerable to Cross-Site Request Forgery in user editing functionality. Malicious attacker can craft special website, which when visited by the victim, will automatically send POST request that deletes given user. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-12382	Improper Limitation of a Pathname 'Path Traversal') vulnerability in Algosec Firewall Analyzer on Linux, 64 bit allows an authenticated user to upload files to a restricted directory leading to code injection. This issue affects Algosec Firewall Analyzer: A33.0 (up to build 320), A33.10 (up to build 210).	N/A	More Details
CVE-2025-40150	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid migrating empty section It reports a bug from device w/ zufs: F2FS-fs (dm-64): Inconsistent segment (173822) type [1, 0] in SSA and SIT F2FS-fs (dm-64): Stopped filesystem due to reason: 4 Thread A Thread B - f2fs_expand_inode_data - f2fs_allocate_pinning_section - f2fs_gc_range - do_garbage_collect w/ segno #x - writepage - f2fs_allocate_data_block - new_curseg - allocate segno #x The root cause is: fallocate on pinning file may race w/ block allocation as above, result in do_garbage_collect() from fallocate() may migrate segment which is just allocated by a log, the log will update segment type in its in-memory structure, however GC will get segment type from on-disk SSA block, once segment type changes by log, we can detect such inconsistency, then shutdown filesystem. In this case, on-disk SSA shows type of segno #173822 is 1 (SUM_TYPE_NODE), however segno #173822 was just allocated as data type segment, so in-memory SIT shows type of segno #173822 is 0 (SUM_TYPE_DATA). Change as below to fix this issue: - check whether current section is empty before gc - add sanity checks on do_garbage_collect() to avoid any race case, result in migrating segment used by log. - btw, it fixes misc issue in printed logs: "SSA and SIT" -> "SIT and SSA".	N/A	More Details
CVE-2025-65015	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. In versions from 1.3.3 to before 1.3.5 and from 1.4.0 to before 1.4.2, the ExceededSizeError exception messages are embedded with non-decoded JWT token parts and may cause Python logging to record an arbitrarily large, forged JWT payload. In situations where a misconfigured — or entirely absent — production-grade web server sits in front of a Python web application, an attacker may be able to send arbitrarily large bearer tokens in the HTTP request headers. When this occurs, Python logging or diagnostic tools (e.g., Sentry) may end up processing extremely large log messages containing the full JWT header during the joserfc.jwt.decode() operation. The same behavior also appears when validating claims and signature payload sizes, as the library raises joserfc.errors.ExceededSizeError() with the full payload embedded in the exception message. Since the payload is already fully loaded into memory at this stage, the library cannot prevent or reject it. This issue has been patched in versions 1.3.5 and 1.4.2.	N/A	More Details
CVE-2025-59113	Windu CMS implements weak client-side brute-force protection by using parameter loginError. Information about attempt count or timeout is not stored on the server, which allows a malicious attacker to bypass this brute-force protection by resetting this parameter. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-40151	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: No support of struct argument in trampoline programs The current implementation does not support struct argument. This causes a oops when running bpf selftest: $ ./test_progs -a tracing_struct Oops[#1]: CPU -1 Unable to handle kernel paging request at virtual address 0000000000000018, era == 9000000085bef268, ra == 90000000844f3938 rcu: INFO: rcu_preempt detected stalls on CPUs/tasks: rcu: 1-...0: (19 ticks this GP) idle=1094/1/0x4000000000000000 softirq=1380/1382 fqs=801 rcu: (detected by 0, t=5252 jiffies, g=1197, q=52 ncpus=4) Sending NMI from CPU 0 to CPUs 1: rcu: rcu_preempt kthread starved for 2495 jiffies! g1197 f0x0 RCU_GP_DOING_FQS(6) ->state=0x0 ->cpu=2 rcu: Unless rcu_preempt kthread gets sufficient CPU time, OOM is now expected behavior. rcu: RCU grace-period kthread stack dump: task:rcu_preempt state:I stack:0 pid:15 tgid:15 ppid:2 task_flags:0x208040 flags:0x00000800 Stack : 9000000100423e80 0000000000000402 0000000000000010 90000001003b0680 9000000085d88000 0000000000000000 0000000000000040 9000000087159350 9000000085c2b9b0 0000000000000001 900000008704a000 0000000000000005 00000000ffff355b 00000000ffff355b 0000000000000000 0000000000000004 9000000085d90510 0000000000000000 0000000000000002 7b5d998f8281e86e 00000000ffff355c 7b5d998f8281e86e 000000000000003f 9000000087159350 900000008715bf98 0000000000000005 9000000087036000 900000008704a000 9000000100407c98 90000001003aff80 900000008715c4c0 9000000085c2b9b0 00000000ffff355b 9000000085c33d3c 00000000000000b4 0000000000000000 9000000007002150 00000000ffff355b 9000000084615480 0000000007000002 ... Call Trace: [<9000000085c2a868>] __schedule+0x410/0x1520 [<9000000085c2b9ac>] schedule+0x34/0x190 [<9000000085c33d38>] schedule_timeout+0x98/0x140 [<90000000845e9120>] rcu_gp_fqs_loop+0x5f8/0x868 [<90000000845ed538>] rcu_gp_kthread+0x260/0x2e0 [<900000008454e8a4>] kthread+0x144/0x238 [<9000000085c26b60>] ret_from_kernel_thread+0x28/0xc8 [<90000000844f20e4>] ret_from_kernel_thread_asm+0xc/0x88 rcu: Stack dump where RCU GP kthread last ran: Sending NMI from CPU 0 to CPUs 2: NMI backtrace for cpu 2 skipped: idling at idle_exit+0x0/0x4 Reject it for now.	N/A	More Details

CVE-2025-40111	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix Use-after-free in validation Nodes stored in the validation duplicates hashtable come from an arena allocator that is cleared at the end of vmw_execbuf_process. All nodes are expected to be cleared in vmw_validation_drop_ht but this node escaped because its resource was destroyed prematurely.	N/A	More Details
CVE-2025-40143	In the Linux kernel, the following vulnerability has been resolved: bpf: dont report verifier bug for missing bpf_scc_visit on speculative path Syzbot generated a program that triggers a verifier_bug() call in maybe_exit_scc(). maybe_exit_scc() assumes that, when called for a state with insn_idx in some SCC, there should be an instance of struct bpf_scc_visit allocated for that SCC. Turns out the assumption does not hold for speculative execution paths. See example in the next patch. maybe_scc_exit() is called from update_branch_counts() for states that reach branch count of zero, meaning that path exploration for a particular path is finished. Path exploration can finish in one of three ways: a. Verification error is found. In this case, update_branch_counts() is called only for non-speculative paths. b. Top level BPF_EXIT is reached. Such instructions are never a part of an SCC, so compute_scc_callchain() in maybe_scc_exit() will return false, and maybe_scc_exit() will return early. c. A checkpoint is reached and matched. Checkpoints are created by is_state_visited(), which calls maybe_enter_scc(), which allocates bpf_scc_visit instances for checkpoints within SCCs. Hence, for non-speculative symbolic execution paths, the assumption still holds: if maybe_scc_exit() is called for a state within an SCC, bpf_scc_visit instance must exist. This patch removes the verifier_bug() call for speculative paths.	N/A	More Details
CVE-2025-41346	Faulty authorization control in software WinPlus v24.11.27 by Informática del Este that allows another user to be impersonated simply by knowing their 'numerical ID', meaning that an attacker could compromise another user's account, thereby affecting the confidentiality, integrity, and availability of the data stored in the application.	N/A	More Details
CVE-2025-65012	Kirby is an open-source content management system. From versions 5.0.0 to 5.1.3, attackers could change the title of any page or the name of any user to a malicious string. Then they could modify any content field of the same model without saving, making the model a candidate for display in the "Changes" dialog. If another authenticated user subsequently opened the dialog in their Panel, the malicious code would be executed. This vulnerability affects all Kirby 5 sites that might have potential attackers in the group of authenticated Panel users or that allow external visitors to update page titles or usernames. The attack requires user interaction by another Panel user and cannot be automated. This issue has been patched in version 5.1.4.	N/A	More Details
CVE-2025-40144	In the Linux kernel, the following vulnerability has been resolved: nvdimm: ndtest: Return -ENOMEM if devm_kcalloc() fails in ndtest_probe() devm_kcalloc() may fail. ndtest_probe() allocates three DMA address arrays (dcr_dma, label_dma, dimm_dma) and later unconditionally uses them in ndtest_nvdimm_init(), which can lead to a NULL pointer dereference under low-memory conditions. Check all three allocations and return -ENOMEM if any allocation fails, jumping to the common error path. Do not emit an extra error message since the allocator already warns on allocation failure.	N/A	More Details
CVE-2025-40142	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: Disable bottom softirqs as part of spin_lock_irq() on PREEMPT_RT snd_pcm_group_lock_irq() acquires a spinlock_t and disables interrupts via spin_lock_irq(). This also implicitly disables the handling of softirqs such as TIMER_SOFTIRQ. On PREEMPT_RT softirqs are preemptible and spin_lock_irq() does not disable them. That means a timer can be invoked during spin_lock_irq() on the same CPU. Due to synchronisations reasons local_bh_disable() has a per-CPU lock named softirq_ctrl.lock which synchronizes individual softirq against each other. syz-bot managed to trigger a lockdep report where softirq_ctrl.lock is acquired in hrtimer_cancel() in addition to hrtimer_run_softirq(). This is a possible deadlock. The softirq_ctrl.lock can not be made part of spin_lock_irq() as this would lead to too much synchronisation against individual threads on the system. To avoid the possible deadlock, softirqs must be manually disabled before the lock is acquired. Disable softirqs before the lock is acquired on PREEMPT_RT.	N/A	More Details
CVE-2025-40141	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: Fix possible UAF on iso_conn_free This attempt to fix similar issue to sco_conn_free where if the conn->sk is not set to NULL may lead to UAF on iso_conn_free.	N/A	More Details
CVE-2025-41348	SQL injection vulnerability in WinPlus v24.11.27 by Informática del Este. This vulnerability allows an attacker recover, create, update an delete databases by sendng a POST request using the parameters 'val1' and 'cont in '/WinplusPortal/ws/sWinplus.svc/json/getacumper_post'.	N/A	More Details
CVE-2025-41349	Stored Cross-site Scripting (XSS)vylnerability type in WinPlus v24.11.27 byInformática del Este that consist of an stored XSS of a stored XSS due to a lack of proper validation of user input by sending a POST request using the 'descripcion' parameter in '/WinplusPortal/ws/sWinplus. svc/json/savesolpla_post'. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	N/A	More Details
CVE-2025-41350	Stored Cross-site Scripting (XSS)vylnerability type in WinPlus v24.11.27 byInformática del Este that consist of an stored XSS of a stored XSS due to a lack of proper validation of user input by sending a POST request using the 'descripcion' parameter in '/WinplusPortal/ws/sWinplus.svc/json/savesoldoc_post'. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie	N/A	More Details

	session details.		
CVE-2025-40140	In the Linux kernel, the following vulnerability has been resolved: net: usb: Remove disruptive netif_wake_queue in rtl8150_set_multicast syzbot reported WARNING in rtl8150_start_xmit/usb_submit_urb. This is the sequence of events that leads to the warning: rtl8150_start_xmit() { netif_stop_queue(); usb_submit_urb(dev->tx_urb); } rtl8150_set_multicast() { netif_stop_queue(); netif_wake_queue(); <-- wakes up TX queue before URB is done } rtl8150_start_xmit() { netif_stop_queue(); usb_submit_urb(dev->tx_urb); <-- double submission } rtl8150_set_multicast being the ndo_set_rx_mode callback should not be calling netif_stop_queue and notif_start_queue as these handle TX queue synchronization. The net core function dev_set_rx_mode handles the synchronization for rtl8150_set_multicast making it safe to remove these locks.	N/A	More Details
CVE-2025-63994	An arbitrary file upload vulnerability in the /php/UploadHandler.php component of RichFilemanager v2.7.6 allows attackers to execute arbitrary code via uploading a crafted file.	N/A	More Details
CVE-2025-40145	In the Linux kernel, the following vulnerability has been resolved: PCI/pwrctrl: Fix double cleanup on devm_add_action_or_reset() failure When devm_add_action_or_reset() fails, it calls the passed cleanup function. Hence the caller must not repeat that cleanup. Replace the "goto err_regulator_free" by the actual freeing, as there will never be a need again for a second user of this label.	N/A	More Details
CVE-2025-41347	Unlimited upload vulnerability for dangerous file types in WinPlus v24.11.27 from Informática del Este. This vulnerability allows an attacker to upload a 'webshell' by sending a POST request to '/WinplusPortal/ws/sWinplus.svc/json/uploadfile'.	N/A	More Details
CVE-2025-40146	In the Linux kernel, the following vulnerability has been resolved: blk-mq: fix potential deadlock while nr_requests grown Allocate and free sched_tags while queue is freezed can deadlock[1], this is a long term problem, hence allocate memory before freezing queue and free memory after queue is unfreezed. [1] https://lore.kernel.org/all/0659ea8d-a463-47c8-9180-43c719e106eb@linux.ibm.com/	N/A	More Details
CVE-2025-40139	In the Linux kernel, the following vulnerability has been resolved: smc: Use __sk_dst_get() and dst_dev_rcu() in in smc_clc_prfx_set(). smc_clc_prfx_set() is called during connect() and not under RCU nor RTNL. Using sk_dst_get(sk)->dev could trigger UAF. Let's use __sk_dst_get() and dev_dst_rcu() under rcu_read_lock() after kernel_getsockname(). Note that the returned value of smc_clc_prfx_set() is not used in the caller. While at it, we change the 1st arg of smc_clc_prfx_set[46]_rcu() not to touch dst there.	N/A	More Details
CVE-2025-64325	Emby Server is a personal media server. Prior to version 4.8.1.0 and prior to Beta version 4.9.0.0-beta, a malicious user can send an authentication request with a manipulated X-Emby-Client value, which gets added to the devices section of the admin dashboard without sanitization. This issue has been patched in version 4.8.1.0 and Beta version 4.9.0.0-beta.	N/A	More Details
CVE-2025-40138	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid NULL pointer dereference in f2fs_check_quota_consistency() syzbot reported a f2fs bug as below: Oops: gen[107.736417][T5848] Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000000: 0000 [#1] SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] CPU: 1 UID: 0 PID: 5848 Comm: syz-executor263 Tainted: G W 6.17.0-rc1-syzkaller-00014-g0e39a731820a #0 PREEMPT_{RT,(full)} RIP: 0010:strcmp+0x3c/0xc0 lib/string.c:284 Call Trace: <TASK> f2fs_check_quota_consistency fs/f2fs/super.c:1188 [inline] f2fs_check_opt_consistency+0x1378/0x2c10 fs/f2fs/super.c:1436 __f2fs_remount fs/f2fs/super.c:2653 [inline] f2fs_reconfigure+0x482/0x1770 fs/f2fs/super.c:5297 reconfigure_super+0x224/0x890 fs/super.c:1077 do_remount fs/namespace.c:3314 [inline] path_mount+0xd18/0xfe0 fs/namespace.c:4112 do_mount fs/namespace.c:4133 [inline] __do_sys_mount fs/namespace.c:4344 [inline] __se_sys_mount+0x317/0x410 fs/namespace.c:4321 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f The direct reason is f2fs_check_quota_consistency() may suffer null-ptr-deref issue in strcmp(). The bug can be reproduced w/ below scripts: mkfs.f2fs -f /dev/vdb mount -t f2fs -o usrquota /dev/vdb /mnt/f2fs quotacheck -uc /mnt/f2fs/ umount /mnt/f2fs mount -t f2fs -o usrjquota=aquota.user,jqfmt=vfsold /dev/vdb /mnt/f2fs mount -t f2fs -o remount,usrjquota=,jqfmt=vfsold /dev/vdb /mnt/f2fs umount /mnt/f2fs So, before old_qname and new_qname comparison, we need to check whether they are all valid pointers, fix it.	N/A	More Details
CVE-2025-40137	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to truncate first page in error path of f2fs_truncate() syzbot reports a bug as below: loop0: detected capacity change from 0 to 40427 F2FS-fs (loop0): Wrong SSA boundary, start(3584) end(4096) blocks(3072) F2FS-fs (loop0): Can't find valid F2FS filesystem in 1th superblock F2FS-fs (loop0): invalid crc value F2FS-fs (loop0): f2fs_convert_inline_folio: corrupted inline inode ino=3, i_addr[0]:0x1601, run fsck to fix. ------------[cut here]------------ kernel BUG at fs/inode.c:753! RIP: 0010:clear_inode+0x169/0x190 fs/inode.c:753 Call Trace: <TASK> evict+0x504/0x9c0 fs/inode.c:810 f2fs_fill_super+0x5612/0x6fa0 fs/f2fs/super.c:5047 get_tree_bdev_flags+0x40e/0x4d0 fs/super.c:1692 vfs_get_tree+0x8f/0x2b0 fs/super.c:1815 do_new_mount+0x2a2/0x9e0 fs/namespace.c:3808 do_mount fs/namespace.c:4136 [inline] __do_sys_mount fs/namespace.c:4347 [inline] __se_sys_mount+0x317/0x410 fs/namespace.c:4324 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f During f2fs_evict_inode(), clear_inode() detects that we missed to truncate all page cache before destorying inode, that is because in below path, we will create page #0 in cache, but missed to drop it in error path, let's	N/A	More Details

	fix it. - evict - f2fs_evict_inode - f2fs_truncate - f2fs_convert_inline_inode - f2fs_grab_cache_folio : create page #0 in cache - f2fs_convert_inline_folio : sanity check failed, return -EFSCORRUPTED - clear_inode detects that inode->i_data.nrpages is not zero		
CVE-2025-40147	In the Linux kernel, the following vulnerability has been resolved: blk-throttle: fix access race during throttle policy activation On repeated cold boots we occasionally hit a NULL pointer crash in blk_should_throtl() when throttling is consulted before the throttle policy is fully enabled for the queue. Checking only q->td != NULL is insufficient during early initialization, so blkg_to_pd() for the throttle policy can still return NULL and blkg_to_tg() becomes NULL, which later gets dereferenced. Unable to handle kernel NULL pointer dereference at virtual address 0000000000000156 ... pc : submit_bio_noacct+0x14c/0x4c8 lr : submit_bio_noacct+0x48/0x4c8 sp : ffff800087f0b690 x29: ffff800087f0b690 x28: 0000000000005f90 x27: ffff00068af393c0 x26: 0000000000080000 x25: 000000000002fbc0 x24: ffff000684ddcc70 x23: 0000000000000000 x22: 0000000000000000 x21: 0000000000000000 x20: 0000000000080000 x19: ffff000684ddcd08 x18: ffffffffffffffff x17: 0000000000000000 x16: ffff80008132a550 x15: 0000ffff98020fff x14: 0000000000000000 x13: 1fffe000d11d7021 x12: ffff000688eb810c x11: ffff00077ec4bb80 x10: ffff000688dcb720 x9 : ffff80008068ef60 x8 : 00000a6fb8a86e85 x7 : 000000000000111e x6 : 0000000000000002 x5 : 0000000000000246 x4 : 0000000000015cff x3 : 0000000000394500 x2 : ffff000682e35e40 x1 : 0000000000364940 x0 : 000000000000001a Call trace: submit_bio_noacct+0x14c/0x4c8 verity_map+0x178/0x2c8 __map_bio+0x228/0x250 dm_submit_bio+0x1c4/0x678 __submit_bio+0x170/0x230 submit_bio_noacct_nocheck+0x16c/0x388 submit_bio_noacct+0x16c/0x4c8 submit_bio+0xb4/0x210 f2fs_submit_read_bio+0x4c/0xf0 f2fs_mpage_readpages+0x3b0/0x5f0 f2fs_readahead+0x90/0xe8 Tighten blk_throtl_activated() to also require that the throttle policy bit is set on the queue: return q->td != NULL && test_bit(blkcg_policy_throtl.plid, q->blkcg_pols); This prevents blk_should_throtl() from accessing throttle group state until policy data has been attached to blkgs.	N/A	More Details
CVE-2025-40152	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix bootup splat with separate_gpu_drm modparam The drm_gem_for_each_gpuvm_bo() call from lookup_vma() accesses drm_gem_obj.gpuva.list, which is not initialized when the drm driver does not support DRIVER_GEM_GPUVA feature. Enable it for msm_kms drm driver to fix the splat seen when msm.separate_gpu_drm=1 modparam is set: [9.506020] Unable to handle kernel paging request at virtual address fffffffffffffff0 [9.523160] Mem abort info: [9.523161] ESR = 0x0000000096000006 [9.523163] EC = 0x25: DABT (current EL), IL = 32 bits [9.523165] SET = 0, FnV = 0 [9.523166] EA = 0, S1PTW = 0 [9.523167] FSC = 0x06: level 2 translation fault [9.523169] Data abort info: [9.523170] ISV = 0, ISS = 0x00000006, ISS2 = 0x00000000 [9.523171] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [9.523172] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [9.523174] swapper pgtable: 4k pages, 48-bit VAs, pgdp=0000000ad370f000 [9.523176] [fffffffffffffff0] pgd=0000000000000000, p4d=0000000ad4787403, pud=0000000ad4788403, pmd=0000000000000000 [9.523184] Internal error: Oops: 0000000096000006 [#1] SMP [9.592968] CPU: 9 UID: 0 PID: 448 Comm: (udev-worker) Not tainted 6.17.0-rc4-assorted-fix-00005-g0e9bb53a2282-dirty #3 PREEMPT [9.592970] Hardware name: Qualcomm CRD, BIOS 6.0.240718.BOOT.MXF.2.4-00515-HAMOA-1 07/18/2024 [9.592971] pstate: a1400005 (NzCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) [9.592973] pc : lookup_vma+0x28/0xe0 [msm] [9.592996] lr : get_vma_locked+0x2c/0x128 [msm] [9.763632] sp : ffff800082dab460 [9.763666] Call trace: [9.763668] lookup_vma+0x28/0xe0 [msm] (P) [9.763688] get_vma_locked+0x2c/0x128 [msm] [9.763706] msm_gem_get_and_pin_iova_range+0x68/0x11c [msm] [9.763723] msm_gem_get_and_pin_iova+0x18/0x24 [msm] [9.763740] msm_fbdev_driver_fbdev_probe+0xd0/0x258 [msm] [9.763760] __drm_fb_helper_initial_config_and_unlock+0x288/0x528 [drm_kms_helper] [9.763771] drm_fb_helper_initial_config+0x44/0x54 [drm_kms_helper] [9.763779] drm_fbdev_client_hotplug+0x84/0xd4 [drm_client_lib] [9.763782] drm_client_register+0x58/0x9c [drm] [9.763806] drm_fbdev_client_setup+0xe8/0xcf0 [drm_client_lib] [9.763809] drm_client_setup+0xb4/0xd8 [drm_client_lib] [9.763811] msm_drm_kms_post_init+0x2c/0x3c [msm] [9.763830] msm_drm_init+0x1a8/0x22c [msm] [9.763848] msm_drm_bind+0x30/0x3c [msm] [9.919273] try_to_bring_up_aggregate_device+0x168/0x1d4 [9.919283] __component_add+0xa4/0x170 [9.919286] component_add+0x14/0x20 [9.919288] msm_dp_display_probe_tail+0x4c/0xac [msm] [9.919315] msm_dp_auxbus_done_probe+0x14/0x20 [msm] [9.919335] dp_aux_ep_probe+0x4c/0xf0 [drm_dp_aux_bus] [9.919341] really_probe+0xbc/0x298 [9.919345] __driver_probe_device+0x78/0x12c [9.919348] driver_probe_device+0x40/0x160 [9.919350] __driver_attach+0x94/0x19c [9.919353] bus_for_each_dev+0x74/0xd4 [9.919355] driver_attach+0x24/0x30 [9.919358] bus_add_driver+0xe4/0x208 [9.919360] driver_register+0x60/0x128 [9.919363] __dp_aux_dp_driver_register+0x24/0x30 [drm_dp_aux_bus] [9.919365] atana33xc20_init+0x20/0x1000 [panel_samsung_atna33xc20] [9.919370] do_one_initcall+0x6c/0x1b0 [9.919374] do_init_module+0x58/0x234 [9.919377] load_module+0x19cc/0x1bd4 [9.919380] init_module_from_file+0x84/0xc4 [9.919382] __arm64_sys_finit_module+0x1b8/0x2cc [9.919384] invoke_syscall+0x48/0x110 [9.919389] el0_svc_common.constprop.0+0xc8/0xe8 [9.919393] do_el0_svc+0x20/0x2c [9.919396] el0_svc+0x34/0xf0 [9.919401] el0t_64_sync_handler+0xa0/0xe4 [9.919403] el0t_64_sync+0x198/0x19c [9.919407] Code: eb0000bf 54000480 d100a003 aa0303e2 (f8418c44) [9.919410] ---[end trace 0000000000000000]--- Patchwork: https://patchwork.freedesktop.org/pa ---truncated---	N/A	More Details
CVE-2025-	Unsafe Deserialization vulnerability in Modular Max Serve before 25.6, specifically when the "--experimental-enable-kvcache-agent" feature is used allowing attackers to execute arbitrary code.	N/A	More Details

60455			
CVE-2025-59115	Windu CMS is vulnerable to Stored Cross-Site Scripting (XSS) in the logon page where input data has no proper validation. Malicious attacker can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting logs page by admin. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-56499	Incorrect access control in mihomo v1.19.11 allows authenticated attackers with low-level privileges to read arbitrary files with elevated privileges via obtaining the external control key from the config file.	N/A	More Details
CVE-2025-34324	GoSign Desktop versions 2.4.0 and earlier use an unsigned update manifest for distributing application updates. The manifest contains package URLs and SHA-256 hashes but is not digitally signed, so its authenticity relies solely on the underlying TLS channel. In affected versions, TLS certificate validation can be disabled when a proxy is configured, allowing an attacker who can intercept network traffic to supply a malicious update manifest and corresponding package with a matching hash. This can cause the client to download and install a tampered update, resulting in arbitrary code execution with the privileges of the GoSign Desktop user on Windows and macOS, or with elevated privileges on some Linux deployments. A local attacker who can modify proxy settings may also abuse this behavior to escalate privileges by forcing installation of a crafted update.	N/A	More Details
CVE-2025-63226	The Sencore SMP100 SMP Media Platform (firmware versions V4.2.160, V60.1.4, V60.1.29) is vulnerable to session hijacking due to improper session management on the /UserManagement.html endpoint. Attackers who are on the same network as the victim and have access to the target's logged-in session can access the endpoint and add new users without any authentication. This allows attackers to gain unauthorized access to the system and perform malicious activities.	N/A	More Details
CVE-2025-40127	In the Linux kernel, the following vulnerability has been resolved: hwrng: ks-sa - fix division by zero in ks_sa_rng_init Fix division by zero in ks_sa_rng_init caused by missing clock pointer initialization. The clk_get_rate() call is performed on an uninitialized clk pointer, resulting in division by zero when calculating delay values. Add clock initialization code before using the clock. drivers/char/hw_random/ks-sa-rng.c | 7 +++++++ 1 file changed, 7 insertions(+)	N/A	More Details
CVE-2025-40126	In the Linux kernel, the following vulnerability has been resolved: sparc: fix accurate exception reporting in copy_{from_to}_user for UltraSPARC The referenced commit introduced exception handlers on user-space memory references in copy_from_user and copy_to_user. These handlers return from the respective function and calculate the remaining bytes left to copy using the current register contents. This commit fixes a couple of bad calculations. This will fix the return value of copy_from_user and copy_to_user in the faulting case. The behaviour of memcpy stays unchanged.	N/A	More Details
CVE-2025-40125	In the Linux kernel, the following vulnerability has been resolved: blk-mq: check kobject state_in_sysfs before deleting in blk_mq_unregister_hctx In __blk_mq_update_nr_hw_queues() the return value of blk_mq_sysfs_register_hctxs() is not checked. If sysfs creation for hctx fails, later changing the number of hw_queues or removing disk will trigger the following warning: kernfs: can not remove 'nr_tags', no directory WARNING: CPU: 2 PID: 637 at fs/kernfs/dir.c:1707 kernfs_remove_by_name_ns+0x13f/0x160 Call Trace: remove_files.isra.1+0x38/0xb0 sysfs_remove_group+0x4d/0x100 sysfs_remove_groups+0x31/0x60 __kobject_del+0x23/0xf0 kobject_del+0x17/0x40 blk_mq_unregister_hctx+0x5d/0x80 blk_mq_sysfs_unregister_hctxs+0x94/0xd0 blk_mq_update_nr_hw_queues+0x124/0x760 nullb_update_nr_hw_queues+0x71/0xf0 [null_blk] nullb_device_submit_queues_store+0x92/0x120 [null_blk] kobjct_del() was called unconditionally even if sysfs creation failed. Fix it by checkig the kobject creation statusbefore deleting it.	N/A	More Details
CVE-2025-40124	In the Linux kernel, the following vulnerability has been resolved: sparc: fix accurate exception reporting in copy_{from_to}_user for UltraSPARC III Anthony Yznaga tracked down that a BUG_ON in ext4 code with large folios enabled resulted from copy_from_user() returning impossibly large values greater than the size to be copied. This lead to __copy_from_iter() returning impossible values instead of the actual number of bytes it was able to copy. The BUG_ON has been reported in https://lore.kernel.org/r/b14f55642207e63e907965e209f6323a0df6dcee.camel@physik.fu-berlin.de The referenced commit introduced exception handlers on user-space memory references in copy_from_user and copy_to_user. These handlers return from the respective function and calculate the remaining bytes left to copy using the current register contents. The exception handlers expect that %o2 has already been masked during the bulk copy loop, but the masking was performed after that loop. This will fix the return value of copy_from_user and copy_to_user in the faulting case. The behaviour of memcpy stays unchanged.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: bpf: Enforce expected_attach_type for tailcall compatibility Yinhao et al. recently reported: Our fuzzer tool discovered an uninitialized pointer issue in the bpf_prog_test_run_xdp() function within the Linux kernel's BPF subsystem. This leads to a NULL pointer dereference when a BPF program attempts to deference the txq member of struct xdp_buff object. The test initializes two programs of BPF_PROG_TYPE_XDP: progA acts as the entry point for bpf_prog_test_run_xdp() and its expected_attach_type can neither be of be BPF_XDP_DEVMAP nor BPF_XDP_CPUMAP. progA calls into a slot of a tailcall map it owns. progB's expected_attach_type must be BPF_XDP_DEVMAP to pass		

CVE-2025-40123	xdp_is_valid_access() validation. The program returns struct xdp_md's egress_ifindex, and the latter is only allowed to be accessed under mentioned expected_attach_type. progB is then inserted into the tailcall which progA calls. The underlying issue goes beyond XDP though. Another example are programs of type BPF_PROG_TYPE_CGROUP_SOCK_ADDR. sock_addr_is_valid_access() as well as sock_addr_func_proto() have different logic depending on the programs' expected_attach_type. Similarly, a program attached to BPF_CGROUP_INET4_GETPEERNAME should not be allowed doing a tailcall into a program which calls bpf_bind() out of BPF which is only enabled for BPF_CGROUP_INET4_CONNECT. In short, specifying expected_attach_type allows to open up additional functionality or restrictions beyond what the basic bpf_prog_type enables. The use of tailcalls must not violate these constraints. Fix it by enforcing expected_attach_type in __bpf_prog_map_compatible(). Note that we only enforce this for tailcall maps, but not for BPF devmaps or cpumaps: There, the programs are invoked through dev_map_bpf_prog_run*() and cpu_map_bpf_prog_run*() which set up a new environment / context and therefore these situations are not prone to this issue.	N/A	More Details
CVE-2025-56643	Requarks Wiki.js 2.5.307 does not properly revoke or invalidate active JWT tokens when a user logs out. As a result, previously issued tokens remain valid and can be reused to access the system, even after logout. This behavior affects session integrity and may allow unauthorized access if a token is compromised. The issue is present in the authentication resolver logic and affects both the GraphQL endpoint and the logout mechanism.	N/A	More Details
CVE-2025-40122	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Fix IA32_PMC_x_CFG_B MSRs access error When running perf_fuzzer on PTL, sometimes the below "unchecked MSR access error" is seen when accessing IA32_PMC_x_CFG_B MSRs. [55.611268] unchecked MSR access error: WRMSR to 0x1986 (tried to write 0x0000000200000001) at rIP: 0xffffffffac564b28 (native_write_msr+0x8/0x30) [55.611280] Call Trace: [55.611282] <TASK> [55.611284] ? intel_pmu_config_acr+0x87/0x160 [55.611289] intel_pmu_enable_acr+0x6d/0x80 [55.611291] intel_pmu_enable_event+0xce/0x460 [55.611293] x86_pmu_start+0x78/0xb0 [55.611297] x86_pmu_enable+0x218/0x3a0 [55.611300] ? x86_pmu_enable+0x121/0x3a0 [55.611302] perf_pmu_enable+0x40/0x50 [55.611307] ctx_resched+0x19d/0x220 [55.611309] __perf_install_in_context+0x284/0x2f0 [55.611311] ? __pfx_remote_function+0x10/0x10 [55.611314] remote_function+0x52/0x70 [55.611317] ? __pfx_remote_function+0x10/0x10 [55.611319] generic_exec_single+0x84/0x150 [55.611323] smp_call_function_single+0xc5/0x1a0 [55.611326] ? __pfx_remote_function+0x10/0x10 [55.611329] perf_install_in_context+0xd1/0x1e0 [55.611331] ? __pfx___perf_install_in_context+0x10/0x10 [55.611333] __do_sys_perf_event_open+0xa76/0x1040 [55.611336] __x64_sys_perf_event_open+0x26/0x30 [55.611337] x64_sys_call+0x1d8e/0x20c0 [55.611339] do_syscall_64+0x4f/0x120 [55.611343] entry_SYSCALL_64_after_hwframe+0x76/0x7e On PTL, GP counter 0 and 1 doesn't support auto counter reload feature, thus it would trigger a #GP when trying to write 1 on bit 0 of CFG_B MSR which requires to enable auto counter reload on GP counter 0. The root cause of causing this issue is the check for auto counter reload (ACR) counter mask from user space is incorrect in intel_pmu_acr_late_setup() helper. It leads to an invalid ACR counter mask from user space could be set into hw.config1 and then written into CFG_B MSRs and trigger the MSR access warning. e.g., User may create a perf event with ACR counter mask (config2=0xcb), and there is only 1 event created, so "cpuc->n_events" is 1. The correct check condition should be "i + idx >= cpuc->n_events" instead of "i + idx > cpuc->n_events" (it looks a typo). Otherwise, the counter mask would traverse twice and an invalid "cpuc->assign[1]" bit (bit 0) is set into hw.config1 and cause MSR accessing error. Besides, also check if the ACR counter mask corresponding events are ACR events. If not, filter out these counter mask. If a event is not a ACR event, it could be scheduled to an HW counter which doesn't support ACR. It's invalid to add their counter index in ACR counter mask. Furthermore, remove the WARN_ON_ONCE() since it's easily triggered as user could set any invalid ACR counter mask and the warning message could mislead users.	N/A	More Details
CVE-2025-40121	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: bytcr_rt5651: Fix invalid quirk input mapping When an invalid value is passed via quirk option, currently bytcr_rt5640 driver just ignores and leaves as is, which may lead to unepxected results like OOB access. This patch adds the sanity check and corrects the input mapping to the certain default value if an invalid value is passed.	N/A	More Details
CVE-2025-63693	The comment editing template (dzz/comment/template/edit_form.htm) in DzzOffice 2.3.x lacks adequate security escaping for user-controllable data in multiple contexts, including HTML and JavaScript strings. This allows low-privilege attackers to construct comment content or request parameters and execute arbitrary JavaScript code when the victim opens the editing pop-up.	N/A	More Details
CVE-2025-40129	In the Linux kernel, the following vulnerability has been resolved: sunrpc: fix null pointer dereference on zero-length checksum In xdr_stream_decode_opaque_auth(), zero-length checksum.len causes checksum.data to be set to NULL. This triggers a NPD when accessing checksum.data in gss_krb5_verify_mic_v2(). This patch ensures that the value of checksum.len is not less than XDR_UNIT.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: net: usb: asix: hold PM usage ref to avoid PM/MDIO + RTNL deadlock Prevent USB runtime PM (autosuspend) for AX88772* in bind. usbnet enables runtime PM (autosuspend) by default, so disabling it via the usb_driver flag is ineffective. On AX88772B, autosuspend shows no measurable power saving with current driver (no link partner, admin up/down). The ~0.453 W -> ~0.248 W drop on v6.1 comes from phylib powering the PHY off on admin-down, not from USB autosuspend. The real hazard is that with runtime PM enabled, ndo_open() (under RTNL) may synchronously		

2025-40120	trigger autoresume (usb_autopm_get_interface()) into asix_resume() while the USB PM lock is held. Resume paths then invoke phylink/phylib and MDIO, which also expect RTNL, leading to possible deadlocks or PM lock vs MDIO wake issues. To avoid this, keep the device runtime-PM active by taking a usage reference in ax88772_bind() and dropping it in unbind(). A non-zero PM usage count blocks runtime suspend regardless of userspace policy (.../power/control - pm_runtime_allow/forbid), making this approach robust against sysfs overrides. Holding a runtime-PM usage ref does not affect system-wide suspend; system sleep/resume callbacks continue to run as before.	N/A	More Details
CVE-2025-40119	In the Linux kernel, the following vulnerability has been resolved: ext4: fix potential null deref in ext4_mb_init() In ext4_mb_init(), ext4_mb_avg_fragment_size_destroy() may be called when sbi->s_mb_avg_fragment_size remains uninitialized (e.g., if groupinfo slab cache allocation fails). Since ext4_mb_avg_fragment_size_destroy() lacks null pointer checking, this leads to a null pointer dereference. == EXT4-fs: no memory for groupinfo slab cache BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: Oops: 0002 [#1] SMP PTI CPU:2 UID: 0 PID: 87 Comm:mount Not tainted 6.17.0-rc2 #1134 PREEMPT(none) RIP: 0010:_raw_spin_lock_irqsave+0x1b/0x40 Call Trace: <TASK> xa_destroy+0x61/0x130 ext4_mb_init+0x483/0x540 __ext4_fill_super+0x116d/0x17b0 ext4_fill_super+0xd3/0x280 get_tree_bdev_flags+0x132/0x1d0 vfs_get_tree+0x29/0xd0 do_new_mount+0x197/0x300 __x64_sys_mount+0x116/0x150 do_syscall_64+0x50/0x1c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e == Therefore, add necessary null check to ext4_mb_avg_fragment_size_destroy() to prevent this issue. The same fix is also applied to ext4_mb_largest_free_orders_destroy().	N/A	More Details
CVE-2025-40118	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Fix array-index-out-of-of-bounds on rmmod Since commit f7b705c238d1 ("scsi: pm80xx: Set phy_attached to zero when device is gone") UBSAN reports: UBSAN: array-index-out-of-bounds in drivers/scsi/pm8001/pm8001_sas.c:786:17 index 28 is out of range for type 'pm8001_phy [16]' on rmmod when using an expander. For a direct attached device, attached_phy contains the local phy id. For a device behind an expander, attached_phy contains the remote phy id, not the local phy id. I.e. while pm8001_ha will have pm8001_ha->chip->n_phy local phys, for a device behind an expander, attached_phy can be much larger than pm8001_ha->chip->n_phy (depending on the amount of phys of the expander). E.g. on my system pm8001_ha has 8 phys with phy ids 0-7. One of the ports has an expander connected. The expander has 31 phys with phy ids 0-30. The pm8001_ha->phy array only contains the phys of the HBA. It does not contain the phys of the expander. Thus, it is wrong to use attached_phy to index the pm8001_ha->phy array for a device behind an expander. Thus, we can only clear phy_attached for devices that are directly attached.	N/A	More Details
CVE-2025-40117	In the Linux kernel, the following vulnerability has been resolved: misc: pci_endpoint_test: Fix array underflow in pci_endpoint_test_ioctl() Commit eefb83790a0d ("misc: pci_endpoint_test: Add doorbell test case") added NO_BAR (-1) to the pci_barno enum which, in practical terms, changes the enum from an unsigned int to a signed int. If the user passes a negative number in pci_endpoint_test_ioctl() then it results in an array underflow in pci_endpoint_test_bar().	N/A	More Details
CVE-2025-40116	In the Linux kernel, the following vulnerability has been resolved: usb: host: max3421-hcd: Fix error pointer dereference in probe cleanup The kthread_run() function returns error pointers so the max3421_hcd->spi_thread pointer can be either error pointers or NULL. Check for both before dereferencing it.	N/A	More Details
CVE-2025-40115	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Fix crash in transport port remove by using ioc_info() During mpt3sas_transport_port_remove(), messages were logged with dev_printk() against &mpt3sas_port->port->dev. At this point the SAS transport device may already be partially unregistered or freed, leading to a crash when accessing its struct device. Using ioc_info(), which logs via the PCI device (ioc->pdev->dev), guaranteed to remain valid until driver removal. [83428.295776] Oops: general protection fault, probably for non-canonical address 0x6f702f323a33312d: 0000 [#1] SMP NOPTI [83428.295785] CPU: 145 UID: 0 PID: 113296 Comm: rmmod Kdump: loaded Tainted: G OE 6.16.0-rc1+ #1 PREEMPT(voluntary) [83428.295792] Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE [83428.295795] Hardware name: Dell Inc. Precision 7875 Tower/, BIOS 89.1.67 02/23/2024 [83428.295799] RIP: 0010:__dev_printk+0x1f/0x70 [83428.295805] Code: 90 90 90 90 90 90 90 90 90 90 0f 1f 44 00 00 49 89 d1 48 85 f6 74 52 4c 8b 46 50 4d 85 c0 74 1f 48 8b 46 68 48 85 c0 74 22 <48> 8b 08 0f b6 7f 01 48 c7 c2 db e8 42 ad 83 ef 30 e9 7b f8 ff ff [83428.295813] RSP: 0018:ff85aeafc3137bb0 EFLAGS: 00010206 [83428.295817] RAX: 6f702f323a33312d RBX: ff4290ee81292860 RCX: 5000cca25103be32 [83428.295820] RDX: ff85aeafc3137bb8 RSI: ff4290eeb1966c00 RDI: ffffffffc1560845 [83428.295823] RBP: ff85aeafc3137c18 R08: 74726f702f303a33 R09: ff85aeafc3137bb8 [83428.295826] R10: ff85aeafc3137b18 R11: ff4290f5bd60fe68 R12: ff4290ee81290000 [83428.295830] R13: ff4290ee6e345de0 R14: ff4290ee81290000 R15: ff4290ee6e345e30 [83428.295833] FS: 00007fd9472a6740(0000) GS:ff4290f5ce96b000(0000) knlGS:0000000000000000 [83428.295837] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [83428.295840] CR2: 00007f242b4db238 CR3: 00000002372b8006 CR4: 0000000000771ef0 [83428.295844] PKRU: 55555554 [83428.295846] Call Trace: [83428.295848] <TASK> [83428.295850] _dev_printk+0x5c/0x80 [83428.295857] ? srso_alias_return_thunk+0x5/0xfbef5 [83428.295863] mpt3sas_transport_port_remove+0x1c7/0x420 [mpt3sas] [83428.295882] _scsih_remove_device+0x21b/0x280 [mpt3sas] [83428.295894] ? _scsih_expander_node_remove+0x108/0x140 [mpt3sas] [83428.295906] ?	N/A	More Details

	srso_alias_return_thunk+0x5/0xfbef5 [83428.295910] mpt3sas_device_remove_by_sas_address.part.0+0x8f/0x110 [mpt3sas] [83428.295921] _scsih_expander_node_remove+0x129/0x140 [mpt3sas] [83428.295933] _scsih_expander_node_remove+0x6a/0x140 [mpt3sas] [83428.295944] scsih_remove+0x3f0/0x4a0 [mpt3sas] [83428.295957] pci_device_remove+0x3b/0xb0 [83428.295962] device_release_driver_internal+0x193/0x200 [83428.295968] driver_detach+0x44/0x90 [83428.295971] bus_remove_driver+0x69/0xf0 [83428.295975] pci_unregister_driver+0x2a/0xb0 [83428.295979] _mpt3sas_exit+0x1f/0x300 [mpt3sas] [83428.295991] __do_sys_delete_module.constprop.0+0x174/0x310 [83428.295997] ? srso_alias_return_thunk+0x5/0xfbef5 [83428.296000] ? __x64_sys_getdents64+0x9a/0x110 [83428.296005] ? srso_alias_return_thunk+0x5/0xfbef5 [83428.296009] ? syscall_trace_enter+0xf6/0x1b0 [83428.296014] do_syscall_64+0x7b/0x2c0 [83428.296019] ? srso_alias_return_thunk+0x5/0xfbef5 [83428.296023] entry_SYSCALL_64_after_hwframe+0x76/0x7e		
CVE-2025-40113	In the Linux kernel, the following vulnerability has been resolved: remoteproc: qcom: pas: Shutdown lite ADSP DTB on X1E The ADSP firmware on X1E has separate firmware binaries for the main firmware and the DTB. The same applies for the "lite" firmware loaded by the boot firmware. When preparing to load the new ADSP firmware we shutdown the lite_pas_id for the main firmware, but we don't shutdown the corresponding lite pas_id for the DTB. The fact that we're leaving it "running" forever becomes obvious if you try to reuse (or just access) the memory region used by the "lite" firmware: The &adsp_boot_mem is accessible, but accessing the &adsp_boot_dtb_mem results in a crash. We don't support reusing the memory regions currently, but nevertheless we should not keep part of the lite firmware running. Fix this by adding the lite_dtb_pas_id and shutting it down as well. We don't have a way to detect if the lite firmware is actually running yet, so ignore the return status of qcom_scm_pas_shutdown() for now. This was already the case before, the assignment to "ret" is not used anywhere.	N/A	More Details
CVE-2025-40112	In the Linux kernel, the following vulnerability has been resolved: sparc: fix accurate exception reporting in copy_{from_to}_user for Niagara The referenced commit introduced exception handlers on user-space memory references in copy_from_user and copy_to_user. These handlers return from the respective function and calculate the remaining bytes left to copy using the current register contents. This commit fixes a couple of bad calculations and a broken epilogue in the exception handlers. This will prevent crashes and ensure correct return values of copy_from_user and copy_to_user in the faulting case. The behaviour of memcpy stays unchanged.	N/A	More Details
CVE-2025-63513	kishan0725 Hospital Management System v4 has an Insecure Direct Object Reference (IDOR) vulnerability in the appointment cancellation functionality.	N/A	More Details
CVE-2025-63225	The Eurolab ELTS100_UBX device (firmware version ELTS100v1.UBX) is vulnerable to Broken Access Control due to missing authentication on critical administrative endpoints. Attackers can directly access and modify sensitive system and network configurations, upload firmware, and execute unauthorized actions without any form of authentication. This vulnerability allows remote attackers to fully compromise the device, control its functionality, and disrupt its operation.	N/A	More Details
CVE-2025-40128	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-63227	The Mozart FM Transmitter web management interface on version WEBMOZZI-00287, contains an unrestricted file upload vulnerability in the /patch.php endpoint. An attacker with administrative credentials can upload arbitrary files (e.g., PHP webshells), which are stored in the /patch/ directory. This allows the attacker to execute arbitrary commands on the server, potentially leading to full system compromise.	N/A	More Details
CVE-2025-63828	Host Header Injection vulnerability in Backdrop CMS 1.32.1 allows attackers to manipulate the Host header in password reset requests, leading to redirects to malicious domains and potential session hijacking via cookie injection.	N/A	More Details
CVE-2025-40134	In the Linux kernel, the following vulnerability has been resolved: dm: fix NULL pointer dereference in __dm_suspend() There is a race condition between dm device suspend and table load that can lead to null pointer dereference. The issue occurs when suspend is invoked before table load completes: BUG: kernel NULL pointer dereference, address: 0000000000000054 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 6 PID: 6798 Comm: dmsetup Not tainted 6.6.0-g7e52f5f0ca9b #62 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 RIP: 0010:blk_mq_wait_quiesce_done+0x0/0x50 Call Trace: <TASK> blk_mq_quiesce_queue+0x2c/0x50 dm_stop_queue+0xd/0x20 __dm_suspend+0x130/0x330 dm_suspend+0x11a/0x180 dev_suspend+0x27e/0x560 ctl_ioctl+0x4cf/0x850 dm_ctl_ioctl+0xd/0x20 vfs_ioctl+0x1d/0x50 __se_sys_ioctl+0x9b/0xc0 __x64_sys_ioctl+0x19/0x30 x64_sys_call+0x2c4a/0x4620 do_syscall_64+0x9e/0x1b0 The issue can be triggered as below: T1 T2 dm_suspend table_load __dm_suspend dm_setup_md_queue dm_mq_init_request_queue blk_mq_init_allocated_queue => q->mq_ops = set->ops; (1) dm_stop_queue / dm_wait_for_completion => q->tag_set NULL pointer! (2) => q->tag_set = set; (3) Fix this by checking if a valid table (map) exists before performing request-based suspend and waiting for target I/O. When map is NULL, skip these table-dependent suspend steps. Even when map is NULL, no I/O can reach any target because there is no table loaded; I/O submitted in this state will fail early in the DM layer. Skipping the table-dependent suspend logic in this case is safe and avoids NULL pointer dereferences.	N/A	More Details

CVE-2025-59116	Windu CMS is vulnerable to User Enumeration. This issue occurs during logon, where a difference in messages could allow an attacker to determine if the login is valid or not, enabling a brute force attack with valid logins. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-64324	KubeVirt is a virtual machine management add-on for Kubernetes. The `hostDisk` feature in KubeVirt allows mounting a host file or directory owned by the user with UID 107 into a VM. However, prior to version 1.6.1 and 1.7.0, the implementation of this feature and more specifically the `DiskOrCreate` option (which creates a file if it doesn't exist) has a logic bug that allows an attacker to read and write arbitrary files owned by more privileged users on the host system. Versions 1.6.1 and 1.7.0 fix the issue.	N/A	More Details
CVE-2025-63695	DzzOffice v2.3.7 and before is vulnerable to Arbitrary File Upload in /dzz/system/ueditor/php/controller.php.	N/A	More Details
CVE-2025-59117	Windu CMS is vulnerable to multiple Stored Cross-Site Scripting (XSS) vulnerabilities in the page editing endpoint windu/admin/content/pages/edit/. This vulnerability can be exploited by a privileged user and may target users with higher privileges. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 4.1 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-40136	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/qm - request reserved interrupt for virtual function The device interrupt vector 3 is an error interrupt for physical function and a reserved interrupt for virtual function. However, the driver has not registered the reserved interrupt for virtual function. When allocating interrupts, the number of interrupts is allocated based on powers of two, which includes this interrupt. When the system enables GICv4 and the virtual function passthrough to the virtual machine, releasing the interrupt in the driver triggers a warning. The WARNING report is: WARNING: CPU: 62 PID: 14889 at arch/arm64/kvm/vgic/vgic-its.c:852 its_free_ite+0x94/0xb4 Therefore, register a reserved interrupt for VF and set the IRQF_NO_AUTOEN flag to avoid that warning.	N/A	More Details
CVE-2025-40135	In the Linux kernel, the following vulnerability has been resolved: ipv6: use RCU in ip6_xmit() Use RCU in ip6_xmit() in order to use dst_dev_rcu() to prevent possible UAF.	N/A	More Details
CVE-2025-12383	In Eclipse Jersey versions 2.45, 3.0.16, 3.1.9 a race condition can cause ignoring of critical SSL configurations - such as mutual authentication, custom key/trust stores, and other security settings. This issue may result in SSLHandshakeException under normal circumstances, but under certain conditions, it could lead to unauthorized trust in insecure servers (see PoC)	N/A	More Details
CVE-2025-58121	Insufficient permission validation on multiple REST API endpoints in Checkmk 2.2.0, 2.3.0, and 2.4.0 before version 2.4.0p16 allows low-privileged users to perform unauthorized actions or obtain sensitive information	N/A	More Details
CVE-2025-58122	Insufficient permission validation in Checkmk 2.4.0 before version 2.4.0p16 allows low-privileged users to modify notification parameters via the REST API, which could lead to unauthorized actions or information disclosure.	N/A	More Details
CVE-2025-63694	DzzOffice v2.3.7 and before is vulnerable to SQL Injection in explorer/groupmanage.	N/A	More Details
CVE-2025-40133	In the Linux kernel, the following vulnerability has been resolved: mptcp: Use __sk_dst_get() and dst_dev_rcu() in mptcp_active_enable(). mptcp_active_enable() is called from subflow_finish_connect(), which is icsk->icsk_af_ops->sk_rx_dst_set() and it's not always under RCU. Using sk_dst_get(sk)->dev could trigger UAF. Let's use __sk_dst_get() and dst_dev_rcu().	N/A	More Details
CVE-2025-40130	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix data race in CPU latency PM QoS request handling The cpu_latency_qos_add/remove/update_request interfaces lack internal synchronization by design, requiring the caller to ensure thread safety. The current implementation relies on the 'pm_qos_enabled' flag, which is insufficient to prevent concurrent access and cannot serve as a proper synchronization mechanism. This has led to data races and list corruption issues. A typical race condition call trace is: [Thread A] ufshcd_pm_qos_exit() --> cpu_latency_qos_remove_request() --> cpu_latency_qos_apply(); --> pm_qos_update_target() --> plist_del <--(1) delete plist node --> memset(req, 0, sizeof(*req)); --> hba->pm_qos_enabled = false; [Thread B] ufshcd_devfreq_target --> ufshcd_devfreq_scale --> ufshcd_scale_clks --> ufshcd_pm_qos_update <--(2) pm_qos_enabled is true --> cpu_latency_qos_update_request --> pm_qos_update_target --> plist_del <--(3) plist node use-after-free Introduces a dedicated mutex to serialize PM QoS operations, preventing data races and ensuring safe access to PM QoS resources, including sysfs interface reads.	N/A	More Details
CVE-	In Ascertia SigningHub through 8.6.8, there is a lack of rate limiting on the invite user function, leading to an		More

2025-54320	email bombing vulnerability. An authenticated attacker can exploit this by automating invite requests.	N/A	Details
CVE-2025-40131	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: Fix peer lookup in ath12k_dp_mon_rx_deliver_msdu() In ath12k_dp_mon_rx_deliver_msdu(), peer lookup fails because rxcb->peer_id is not updated with a valid value. This is expected in monitor mode, where RX frames bypass the regular RX descriptor path that typically sets rxcb->peer_id. As a result, the peer is NULL, and link_id and link_valid fields in the RX status are not populated. This leads to a WARN_ON in mac80211 when it receives data frame from an associated station with invalid link_id. Fix this potential issue by using ppduinfo->peer_id, which holds the correct peer id for the received frame. This ensures that the peer is correctly found and the associated link metadata is updated accordingly. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.4.1-00199-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2025-64996	In Checkmk versions prior to 2.4.0p16, 2.3.0p41, and all versions of 2.2.0 and older, the mk_inotify plugin creates world-readable and writable files, allowing any local user on the system to read the plugin's output and manipulate it, potentially leading to unauthorized access to or modification of monitoring data.	N/A	More Details
CVE-2025-9977	Value provided in one of POST parameters sent during the process of logging in to Times Software E-Payroll is not sanitized properly, which allows an unauthenticated attacker to perform DoS attacks. SQL injection attacks might also be feasible, although so far creating a working exploit has been prevented probably by backend filtering mechanisms. Additionally, command injection attempts cause the application to return extensive error messages disclosing some information about the internal infrastructure. Patching status is unknown because the vendor has not replied to messages sent by the CNA.	N/A	More Details
CVE-2025-63229	The Mozart FM Transmitter web management interface on version WEBMOZZI-00287, contains a reflected Cross-Site Scripting (XSS) vulnerability in the /main0.php endpoint. By injecting a malicious JavaScript payload into the ?m= query parameter, an attacker can execute arbitrary code in the victim's browser, potentially stealing sensitive information, hijacking sessions, or performing unauthorized actions.	N/A	More Details
CVE-2025-63217	The Itel DAB MUX (IDMUX build c041640a) is vulnerable to Authentication Bypass due to improper JWT validation across devices. Attackers can reuse a valid JWT token obtained from one device to authenticate and gain administrative access to any other device running the same firmware, even if the passwords and networks are different. This allows full compromise of affected devices.	N/A	More Details
CVE-2025-63216	The Itel DAB Gateway (IDGat build c041640a) is vulnerable to Authentication Bypass due to improper JWT validation across devices. Attackers can reuse a valid JWT token obtained from one device to authenticate and gain administrative access to any other device running the same firmware, even if the passwords and networks are different. This allows full compromise of affected devices.	N/A	More Details
CVE-2025-63215	The Sound4 IMPACT web-based management interface is vulnerable to Remote Code Execution (RCE) via a malicious firmware update package. The update mechanism fails to validate the integrity of manual.sh, allowing an attacker to inject arbitrary commands by modifying this script and repackaging the firmware.	N/A	More Details
CVE-2025-54321	In Ascertia SigningHub through 8.6.8, there is a lack of rate limiting on the reset password function, leading to an email bombing vulnerability. An authenticated attacker can exploit this by automating reset password requests.	N/A	More Details
CVE-2025-63228	The Mozart FM Transmitter web management interface on version WEBMOZZI-00287, contains an unauthenticated file upload vulnerability in the /upload_file.php endpoint. An attacker can exploit this by sending a crafted POST request with a malicious file (e.g., a PHP webshell) to the server. The uploaded file is stored in the /upload/ directory, enabling remote code execution and full system compromise.	N/A	More Details
CVE-2025-40132	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: sof_sdw: Prevent jump to NULL add_sidecar callback In create_sdw_dailink() check that sof_end->codec_info->add_sidecar is not NULL before calling it. The original code assumed that if include_sidecar is true, the codec on that link has an add_sidecar callback. But there could be other codecs on the same link that do not have an add_sidecar callback.	N/A	More Details
CVE-2024-21635	Memos is a privacy-first, lightweight note-taking service that uses Access Tokens to authenticate application access. When a user changes their password, the existing list of Access Tokens stay valid instead of expiring. If a user finds that their account has been compromised, they can update their password. In versions up to and including 0.18.1, though, the bad actor will still have access to their account because the bad actor's Access Token stays on the list as a valid token. The user will have to manually delete the bad actor's Access Token to secure their account. The list of Access Tokens has a generic Description which makes it hard to pinpoint a bad actor in a list of Access Tokens. A known patched version of Memos isn't available. To improve Memos security, all Access Tokens will need to be revoked when a user changes their password. This removes the session for all the user's devices and prompts the user to log in again. One can treat the old Access Tokens as "invalid" because those Access Tokens were created with the older password.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mm: hugetlb: avoid soft lockup when mprotect to large memory area When calling mprotect() to a large hugetlb memory area in our customer's workload (~300GB hugetlb memory), soft lockup was observed: watchdog: BUG: soft lockup - CPU#98 stuck for 23s! [t2_new_sysv:126916] CPU: 98 PID: 126916 Comm: t2_new_sysv Kdump: loaded Not tainted 6.17-rc7		

CVE-2025-40153	Hardware name: GIGACOMPUTING R2A3-T40-AAV1/Jefferson CIO, BIOS 5.4.4.1 07/15/2025 pstate: 20400009 (nzCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mte_clear_page_tags+0x14/0x24 lr : mte_sync_tags+0x1c0/0x240 sp : ffff80003150bb80 x29: ffff80003150bb80 x28: ffff00739e9705a8 x27: 0000ffd2d6a00000 x26: 0000ff8e4bc00000 x25: 00e80046cde00f45 x24: 0000000000022458 x23: 0000000000000000 x22: 0000000000000004 x21: 000000011b380000 x20: ffff000000000000 x19: 000000011b379f40 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : ffffc875e0aa5e2c x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : fffffc01ce7a5c00 x4 : 00000000046cde00 x3 : fffffc0000000000 x2 : 0000000000000004 x1 : 0000000000000040 x0 : ffff0046cde7c000 Call trace: mte_clear_page_tags+0x14/0x24 set_huge_pte_at+0x25c/0x280 hugetlb_change_protection+0x220/0x430 change_protection+0x5c/0x8c mprotect_fixup+0x10c/0x294 do_mprotect_pkey.constprop.0+0x2e0/0x3d4 __arm64_sys_mprotect+0x24/0x44 invoke_syscall+0x50/0x160 el0_svc_common+0x48/0x144 do_el0_svc+0x30/0xe0 el0_svc+0x30/0xf0 el0t_64_sync_handler+0xc4/0x148 el0t_64_sync+0x1a4/0x1a8 Soft lockup is not triggered with THP or base page because there is cond_resched() called for each PMD size. Although the soft lockup was triggered by MTE, it should be not MTE specific. The other processing which takes long time in the loop may trigger soft lockup too. So add cond_resched() for hugetlb to avoid soft lockup.	N/A	More Details
CVE-2025-12703	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-12784	Certain HP LaserJet Pro printers may be vulnerable to information disclosure leading to credential exposure by altering the scan/send destination address and/or modifying the LDAP Server.	N/A	More Details
CVE-2025-64717	ZITADEL is an open source identity management platform. Starting in version 2.50.0 and prior to versions 2.71.19, 3.4.4, and 4.6.6, a vulnerability in ZITADEL's federation process allowed auto-linking users from external identity providers to existing users in ZITADEL even if the corresponding IdP was not active or if the organization did not allow federated authentication. This vulnerability stems from the platform's failure to correctly check or enforce an organization's specific security settings during the authentication flow. An Organization Administrator can explicitly disable an IdP or disallow federation, but this setting was not being honored during the auto-linking process. This allowed an unauthenticated attacker to initiate a login using an IdP that should have been disabled for that organization. The platform would incorrectly validate the login and, based on a matching criteria, link the attacker's external identity to an existing internal user account. This may result in a full Account Takeover, bypassing the organization's mandated security controls. Note that accounts with MFA enabled can not be taken over by this attack. Also note that only IdPs create on an instance level would allow this to work. IdPs registered on another organization would always be denied in the (auto-)linking process. Versions 4.6.6, 3.4.4, and 2.71.19 resolve the issue by correctly validating the organization's login policy before auto-linking an external user. No known workarounds are available aside from upgrading.	N/A	More Details
CVE-2025-2448	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-41069	Insecure Direct Object Reference (IDOR) vulnerability in DeporSite of T-INNOVA. This vulnerability allows an attacker to access or modify unauthorized resources by manipulating requests using the 'idUsuario' parameter in ‘/ajax/TInnova_v2/Formulario_Consentimiento/llamadaAjax/obtenerDatosConsentimientos’, which could lead to the exposure or alteration os confidential data.	N/A	More Details
CVE-2025-40681	Cross-site Scripting (XSS) vulnerability reflected in xCally's Omnichannel v3.30.1. This vulnerability allowsan attacker to executed JavaScript code in the victim's browser by sending them a malicious URL using the 'failureMessage' parameter in '/login'. This vulnerability can be exploited to steal sentitive user data, such as session cookies , or to perform actions on behalf of the user.	N/A	More Details
CVE-2025-64384	Missing Authorization vulnerability in jetmonsters JetFormBuilder jetformbuilder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JetFormBuilder: from n/a through <= 3.5.3.	N/A	More Details
CVE-2025-64292	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PascalBajorat Analytics Germanized for Google Analytics ga-germanized allows DOM-Based XSS.This issue affects Analytics Germanized for Google Analytics: from n/a through <= 1.6.2.	N/A	More Details
CVE-2025-10460	A SQL Injection vulnerability on an endpoint in BEIMS Contractor Web, a legacy product that is no longer maintained or patched by the vendor, allows an unauthorised user to retrieve sensitive database contents via unsanitized parameter input. This vulnerability occurs due to improper input validation on /BEIMSWeb/contractor.asp endpoint and successful exploitation requires a contractor.asp endpoint open to the internet. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity and potentially the availability of the database. Version 5.7.139 has been confirmed	N/A	More Details

	as vulnerable. Other versions have not been confirmed by the vendor and users should assume that all versions of BEIMS Contractor Web may be impacted until further guidance is provided by the vendor.		
CVE-2025-60022	Improper certificate validation vulnerability exists in 'デジラアプリ' App for iOS prior to ver.80.10.00. If this vulnerability is exploited, a man-in-the-middle attack may allow an attacker to eavesdrop on and/or tamper with an encrypted communication.	N/A	More Details
CVE-2025-64716	Anubis is a Web AI Firewall Utility that challenges users' connections in order to protect upstream resources from scraper bots. Prior to version 1.23.0, when using subrequest authentication, Anubis did not perform validation of the redirect URL and redirects user to any URL scheme. While most modern browsers do not allow a redirect to `javascript:` URLs, it could still trigger dangerous behavior in some cases. Anybody with a subrequest authentication may be affected. Version 1.23.0 contains a fix for the issue.	N/A	More Details
CVE-2025-64710	Bitplatform Boilerplate is a Visual studio and .NET project template. Versions prior to 9.11.3 are affected by a cross-site scripting (XSS) vulnerability in the WebInteropApp/WebAppInterop, potentially allowing attackers to inject malicious scripts that compromise the security and integrity of web applications. Applications based on this Bitplatform Boilerplate might also be vulnerable. Version 9.11.3 fixes the issue.	N/A	More Details
CVE-2025-59367	An authentication bypass vulnerability has been identified in certain DSL series routers, may allow remote attackers to gain unauthorized access into the affected system. Refer to the 'Security Update for DSL Series Router' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-64523	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. Versions prior to 2.45.1 have an Insecure Direct Object Reference (IDOR) vulnerability in the FileBrowser application's share deletion functionality. This vulnerability allows any authenticated user with share permissions to delete other users' shared links without authorization checks. The impact is significant as malicious actors can disrupt business operations by systematically removing shared files and links. This leads to denial of service for legitimate users, potential data loss in collaborative environments, and breach of data confidentiality agreements. In organizational settings, this could affect critical file sharing for projects, presentations, or document collaboration. Version 2.45.1 contains a fix for the issue.	N/A	More Details
CVE-2025-11681	Denial-of-service condition in M-Files Server versions before 25.11.15392.1, before 25.2 LTS SR2 and before 25.8 LTS SR2 allows an authenticated user to cause the MFserver process to crash.	N/A	More Details
CVE-2025-64429	DuckDB is a SQL database management system. DuckDB implemented block-based encryption of DB on the filesystem starting with DuckDB 1.4.0. There are a few issues related to this implementation. The DuckDB can fall back to an insecure random number generator (pcg32) to generate cryptographic keys or IVs. When clearing keys from memory, the compiler may remove the memset() and leave sensitive data on the heap. By modifying the database header, an attacker could downgrade the encryption mode from GCM to CTR to bypass integrity checks. There may be a failure to check return value on call to OpenSSL `rand_bytes()`. An attacker could use public IVs to compromise the internal state of RNG and determine the randomly generated key used to encrypt temporary files, get access to cryptographic keys if they have access to process memory (e.g. through memory leak),circumvent GCM integrity checks, and/or influence the OpenSSL random number generator and DuckDB would not be able to detect a failure of the generator. Version 1.4.2 has disabled the insecure random number generator by no longer using the fallback to write to or create databases. Instead, DuckDB will now attempt to install and load the OpenSSL implementation in the `httpfs` extension. DuckDB now uses secure MbedTLS primitive to clear memory as recommended and requires explicit specification of ciphers without integrity checks like CTR on `ATTACH`. Additionally, DuckDB now checks the return code.	N/A	More Details
CVE-2025-40154	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: bytcr_rt5640: Fix invalid quirk input mapping When an invalid value is passed via quirk option, currently bytcr_rt5640 driver only shows an error message but leaves as is. This may lead to unepxected results like OOB access. This patch corrects the input mapping to the certain default value if an invalid value is passed.	N/A	More Details
CVE-2025-13310	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-4321	In a Bluetooth device, using RS9116-WiseConnect SDK experiences a Denial of Service, if it receives malformed L2CAP packets, only hard reset will bring the device to normal operation	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: media: iris: fix module removal if firmware download failed Fix remove if firmware failed to load: qcom-iris aa00000.video-codec: Direct firmware load for qcom/vpu/vpu33_p4.mbn failed with error -2 qcom-iris aa00000.video-codec: firmware download failed qcom-iris aa00000.video-codec: core init failed then: $ echo aa00000.video-codec > /sys/bus/platform/drivers/qcom-iris/unbind Triggers: genpd genpd:1:aa00000.video-codec: Runtime PM usage count underflow! ----------[cut here]---------- video_cc_mvs0_clk already disabled WARNING: drivers/clk/clk.c:1206 at clk_core_disable+0xa4/0xac, CPU#1: sh/542 <snip> pc :		

CVE-2025-40208	clk_core_disable+0xa4/0xac lr : clk_core_disable+0xa4/0xac <snip> Call trace: clk_core_disable+0xa4/0xac (P) clk_disable+0x30/0x4c iris_disable_unprepare_clock+0x20/0x48 [qcom_iris] iris_vpu_power_off_hw+0x48/0x58 [qcom_iris] iris_vpu33_power_off_hardware+0x44/0x230 [qcom_iris] iris_vpu_power_off+0x34/0x84 [qcom_iris] iris_core_deinit+0x44/0xc8 [qcom_iris] iris_remove+0x20/0x48 [qcom_iris] platform_remove+0x20/0x30 device_remove+0x4c/0x80 <snip> ---[end trace 0000000000000000]--- ------------[cut here]------------ video_cc_mvs0_clk already unprepared WARNING: drivers/clk/clk.c:1065 at clk_core_unprepare+0xf0/0x110, CPU#2: sh/542 <snip> pc : clk_core_unprepare+0xf0/0x110 lr : clk_core_unprepare+0xf0/0x110 <snip> Call trace: clk_core_unprepare+0xf0/0x110 (P) clk_unprepare+0x2c/0x44 iris_disable_unprepare_clock+0x28/0x48 [qcom_iris] iris_vpu_power_off_hw+0x48/0x58 [qcom_iris] iris_vpu33_power_off_hardware+0x44/0x230 [qcom_iris] iris_vpu_power_off+0x34/0x84 [qcom_iris] iris_core_deinit+0x44/0xc8 [qcom_iris] iris_remove+0x20/0x48 [qcom_iris] platform_remove+0x20/0x30 device_remove+0x4c/0x80 <snip> ---[end trace 0000000000000000]--- genpd genpd:0:aa00000.video-codec: Runtime PM usage count underflow! ------------[cut here]------------ gcc_video_axi0_clk already disabled WARNING: drivers/clk/clk.c:1206 at clk_core_disable+0xa4/0xac, CPU#4: sh/542 <snip> pc : clk_core_disable+0xa4/0xac lr : clk_core_disable+0xa4/0xac <snip> Call trace: clk_core_disable+0xa4/0xac (P) clk_disable+0x30/0x4c iris_disable_unprepare_clock+0x20/0x48 [qcom_iris] iris_vpu33_power_off_controller+0x17c/0x428 [qcom_iris] iris_vpu_power_off+0x48/0x84 [qcom_iris] iris_core_deinit+0x44/0xc8 [qcom_iris] iris_remove+0x20/0x48 [qcom_iris] platform_remove+0x20/0x30 device_remove+0x4c/0x80 <snip> ------------[cut here]------------ gcc_video_axi0_clk already unprepared WARNING: drivers/clk/clk.c:1065 at clk_core_unprepare+0xf0/0x110, CPU#4: sh/542 <snip> pc : clk_core_unprepare+0xf0/0x110 lr : clk_core_unprepare+0xf0/0x110 <snip> Call trace: clk_core_unprepare+0xf0/0x110 (P) clk_unprepare+0x2c/0x44 iris_disable_unprepare_clock+0x28/0x48 [qcom_iris] iris_vpu33_power_off_controller+0x17c/0x428 [qcom_iris] iris_vpu_power_off+0x48/0x84 [qcom_iris] iris_core_deinit+0x44/0xc8 [qcom_iris] iris_remove+0x20/0x48 [qcom_iris] platform_remove+0x20/0x30 device_remove+0x4c/0x80 <snip> ---[end trace 0000000000000000]--- Skip deinit if initialization never succeeded.	N/A	More Details
CVE-2025-40207	In the Linux kernel, the following vulnerability has been resolved: media: v4l2-subdev: Fix alloc failure check in v4l2_subdev_call_state_try() v4l2_subdev_call_state_try() macro allocates a subdev state with __v4l2_subdev_state_alloc(), but does not check the returned value. If __v4l2_subdev_state_alloc fails, it returns an ERR_PTR, and that would cause v4l2_subdev_call_state_try() to crash. Add proper error handling to v4l2_subdev_call_state_try().	N/A	More Details
CVE-2025-40206	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_objref: validate objref and objrefmap expressions Referencing a synproxy stateful object from OUTPUT hook causes kernel crash due to infinite recursive calls: BUG: TASK stack guard page was hit at 000000008bda5b8c (stack is 000000003ab1c4a5..00000000494d8b12) [...] Call Trace: __find_rr_leaf+0x99/0x230 fib6_table_lookup+0x13b/0x2d0 ip6_pol_route+0xa4/0x400 fib6_rule_lookup+0x156/0x240 ip6_route_output_flags+0xc6/0x150 __nf_ip6_route+0x23/0x50 synproxy_send_tcp_ipv6+0x106/0x200 synproxy_send_client_synack_ipv6+0x1aa/0x1f0 nft_synproxy_do_eval+0x263/0x310 nft_do_chain+0x5a8/0x5f0 [nf_tables nft_do_chain_inet+0x98/0x110 nf_hook_slow+0x43/0xc0 __ip6_local_out+0xf0/0x170 ip6_local_out+0x17/0x70 synproxy_send_tcp_ipv6+0x1a2/0x200 synproxy_send_client_synack_ipv6+0x1aa/0x1f0 [...] Implement objref and objrefmap expression validate functions. Currently, only NFT_OBJECT_SYNPROXY object type requires validation. This will also handle a jump to a chain using a synproxy object from the OUTPUT hook. Now when trying to reference a synproxy object in the OUTPUT hook, nft will produce the following error: synproxy_crash.nft: Error: Could not process rule: Operation not supported synproxy name mysynproxy ^^^^^^^^^^^^^^^^^^^^^^^^^^	N/A	More Details
CVE-2025-40205	In the Linux kernel, the following vulnerability has been resolved: btrfs: avoid potential out-of-bounds in btrfs_encode_fh() The function btrfs_encode_fh() does not properly account for the three cases it handles. Before writing to the file handle (fh), the function only returns to the user BTRFS_FID_SIZE_NON_CONNECTABLE (5 dwords, 20 bytes) or BTRFS_FID_SIZE_CONNECTABLE (8 dwords, 32 bytes). However, when a parent exists and the root ID of the parent and the inode are different, the function writes BTRFS_FID_SIZE_CONNECTABLE_ROOT (10 dwords, 40 bytes). If *max_len is not large enough, this write goes out of bounds because BTRFS_FID_SIZE_CONNECTABLE_ROOT is greater than BTRFS_FID_SIZE_CONNECTABLE originally returned. This results in an 8-byte out-of-bounds write at fid->parent_root_objectid = parent_root_id. A previous attempt to fix this issue was made but was lost. https://lore.kernel.org/all/4CADAEEC020000780001B32C@vpn.id2.novell.com/ Although this issue does not seem to be easily triggerable, it is a potential memory corruption bug that should be fixed. This patch resolves the issue by ensuring the function returns the appropriate size for all three cases and validates that *max_len is large enough before writing any data.	N/A	More Details
CVE-2025-40204	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix MAC comparison to be constant-time To prevent timing attacks, MACs need to be compared in constant time. Use the appropriate helper function for this.	N/A	More Details
CVE-2025-40203	In the Linux kernel, the following vulnerability has been resolved: listmount: don't call path_put() under namespace semaphore Massage listmount() and make sure we don't call path_put() under the namespace semaphore. If we put the last reference we're fscked.	N/A	More Details

CVE-2025-40202	In the Linux kernel, the following vulnerability has been resolved: ipmi: Rework user message limit handling The limit on the number of user messages had a number of issues, improper counting in some cases and a use after free. Restructure how this is all done to handle more in the receive message allocation routine, so all refcouting and user message limit counts are done in that routine. It's a lot cleaner and safer.	N/A	More Details
CVE-2025-40201	In the Linux kernel, the following vulnerability has been resolved: kernel/sys.c: fix the racy usage of task_lock(tsk->group_leader) in sys_prlimit64() paths The usage of task_lock(tsk->group_leader) in sys_prlimit64()->do_prlimit() path is very broken. sys_prlimit64() does get_task_struct(tsk) but this only protects task_struct itself. If tsk != current and tsk is not a leader, this process can exit/exec and task_lock(tsk->group_leader) may use the already freed task_struct. Another problem is that sys_prlimit64() can race with mt-exec which changes ->group_leader. In this case do_prlimit() may take the wrong lock, or (worse) ->group_leader may change between task_lock() and task_unlock(). Change sys_prlimit64() to take tasklist_lock when necessary. This is not nice, but I don't see a better fix for -stable.	N/A	More Details
CVE-2025-40200	In the Linux kernel, the following vulnerability has been resolved: Squashfs: reject negative file sizes in squashfs_read_inode() Syskaller reports a "WARNING in ovl_copy_up_file" in overlayfs. This warning is ultimately caused because the underlying Squashfs file system returns a file with a negative file size. This commit checks for a negative file size and returns EINVAL. [phillip@squashfs.org.uk: only need to check 64 bit quantity]	N/A	More Details
CVE-2025-40199	In the Linux kernel, the following vulnerability has been resolved: page_pool: Fix PP_MAGIC_MASK to avoid crashing on some 32-bit arches Helge reported that the introduction of PP_MAGIC_MASK let to crashes on boot on his 32-bit parisc machine. The cause of this is the mask is set too wide, so the page_pool_page_is_pp() incurs false positives which crashes the machine. Just disabling the check in page_pool_is_pp() will lead to the page_pool code itself malfunctioning; so instead of doing this, this patch changes the define for PP_DMA_INDEX_BITS to avoid mistaking arbitrary kernel pointers for page_pool-tagged pages. The fix relies on the kernel pointers that alias with the pp_magic field always being above PAGE_OFFSET. With this assumption, we can use the lowest bit of the value of PAGE_OFFSET as the upper bound of the PP_DMA_INDEX_MASK, which should avoid the false positives. Because we cannot rely on PAGE_OFFSET always being a compile-time constant, nor on it always being >0, we fall back to disabling the dma_index storage when there are not enough bits available. This leaves us in the situation we were in before the patch in the Fixes tag, but only on a subset of architecture configurations. This seems to be the best we can do until the transition to page types in complete for page_pool pages. v2: - Make sure there's at least 8 bits available and that the PAGE_OFFSET bit calculation doesn't wrap	N/A	More Details
CVE-2025-40198	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid potential buffer over-read in parse_apply_sb_mount_options() Unlike other strings in the ext4 superblock, we rely on tune2fs to make sure s_mount_opts is NUL terminated. Harden parse_apply_sb_mount_options() by treating s_mount_opts as a potential __nonstring.	N/A	More Details
CVE-2025-40197	In the Linux kernel, the following vulnerability has been resolved: media: mc: Clear minor number before put device The device minor should not be cleared after the device is released.	N/A	More Details
CVE-2025-65072	Rejected reason: Not used	N/A	More Details
CVE-2025-65071	Rejected reason: Not used	N/A	More Details
CVE-2025-65070	Rejected reason: Not used	N/A	More Details
CVE-2025-65069	Rejected reason: Not used	N/A	More Details
CVE-2025-64444	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in NCP-HG100 1.4.48.16 and earlier. If exploited, a remote attacker who has obtained the authentication information to log in to the management page of the product may execute an arbitrary OS command with root privileges.	N/A	More Details
CVE-2025-12897	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-4616	An insufficient validation of an untrusted input vulnerability in Palo Alto Networks Prisma® Browser allows a locally authenticated non-admin user to revert the browser’s security controls.	N/A	More Details

CVE-2025-4617	An insufficient policy enforcement vulnerability in Palo Alto Networks Prisma® Browser on Windows allows a locally authenticated non-admin user to bypass the screenshot control feature of the browser. Browser self-protection should be enabled to mitigate this issue.	N/A	More Details
CVE-2025-4618	A sensitive information disclosure vulnerability in Palo Alto Networks Prisma® Browser allows a locally authenticated non-admin user to retrieve sensitive data from Prisma Browser. Browser self-protection should be enabled to mitigate this issue.	N/A	More Details
CVE-2025-40110	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix a null-ptr access in the cursor snooper Check that the resource which is converted to a surface exists before trying to use the cursor snooper on it. vmw_cmd_res_check allows explicit invalid (SVGA3D_INVALID_ID) identifiers because some svga commands accept SVGA3D_INVALID_ID to mean "no surface", unfortunately functions that accept the actual surfaces as objects might (and in case of the cursor snooper, do not) be able to handle null objects. Make sure that we validate not only the identifier (via the vmw_cmd_res_check) but also check that the actual resource exists before trying to do something with it. Fixes unchecked null-ptr reference in the snooping code.	N/A	More Details
CVE-2025-64754	Jitsi Meet is an open source video conferencing application. A vulnerability present in versions prior to 2.0.10532 allows attackers to hijack the OAuth authentication window for Microsoft accounts. This is fixed in version 2.0.10532. No known workarounds are available.	N/A	More Details
CVE-2025-12187	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-4619	A denial-of-service (DoS) vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to reboot a firewall by sending a specially crafted packet through the dataplane. Repeated attempts to initiate a reboot causes the firewall to enter maintenance mode. This issue is applicable to the PAN-OS software versions listed below on PA-Series firewalls, VM-Series firewalls, and Prisma® Access software. This issue does not affect Cloud NGFW. We have successfully completed the Prisma Access upgrade for all customers, with the exception of those facing issues such as conflicting maintenance windows. Remaining customers will be promptly scheduled for an upgrade through our standard upgrade process.	N/A	More Details
CVE-2016-15056	Ubee EVW3226 cable modem/routers firmware versions up to and including 1.0.20 store configuration backup files in the web root after they are generated for download. These backup files remain accessible without authentication until the next reboot. A remote attacker on the local network can request 'Configuration_file.cfg' directly to obtain the backup archive. Because backup files are not encrypted, they expose sensitive information including the plaintext admin password, allowing full compromise of the device.	N/A	More Details
CVE-2018-25125	Netis ADSL Router DL4322D firmware RTK 2.1.1 contains a buffer overflow vulnerability in the embedded FTP service that allows an authenticated remote user to trigger a denial of service. After logging in to the FTP service, sending an FTP command such as ABOR with an excessively long argument causes the service, and in practice the router, to crash or become unresponsive, resulting in a loss of availability for the device and connected users.	N/A	More Details
CVE-2021-4465	ReQuest Serious Play F3 Media Server versions 7.0.3.4968 (Pro), 7.0.2.4954, 6.5.2.4954, 6.4.2.4681, 6.3.2.4203, and 2.0.1.823 contain a remote denial-of-service vulnerability. The device can be shut down or rebooted by an unauthenticated attacker through a single crafted HTTP GET request, allowing remote interruption of service availability.	N/A	More Details
CVE-2021-4466	IPCop versions up to and including 2.1.9 contain an authenticated remote code execution vulnerability within the web-based administration interface. The email configuration component inserts user-controlled values, including the EMAIL_PW parameter, directly into system-level operations without proper input sanitation. By modifying the email password field to include shell metacharacters and issuing a save-and-test-mail action, an authenticated attacker can execute arbitrary operating system commands with the privileges of the web interface, resulting in full system compromise.	N/A	More Details
CVE-2021-4467	Positive Technologies MaxPatrol 8 and XSpider contain a remote denial-of-service vulnerability in the client communication service on TCP port 2002. The service generates a new session identifier for each incoming connection without adequately limiting concurrent requests. An unauthenticated remote attacker can repeatedly issue HTTPS requests to the service, causing excessive allocation of session identifiers. Under load, session identifier collisions may occur, forcing active client sessions to disconnect and resulting in service disruption.	N/A	More Details
CVE-2021-4468	PLANEX CS-QP50F-ING2 smart cameras expose a configuration backup interface over HTTP that does not require authentication. A remote, unauthenticated attacker can directly retrieve a compressed configuration backup file from the device. The backup contains sensitive configuration information, including credentials, allowing an attacker to obtain administrative access to the camera and compromise the confidentiality of the monitored environment.	N/A	More Details
CVE-	Denver SHO-110 IP cameras expose a secondary HTTP service on TCP port 8001 that provides access to a '/snapshot' endpoint without authentication. While the primary web interface on port 80 enforces		

2021-4469	authentication, the backdoor service allows any remote attacker to retrieve image snapshots by directly requesting the 'snapshot' endpoint. An attacker can repeatedly collect snapshots and reconstruct the camera stream, compromising the confidentiality of the monitored environment.	N/A	More Details
CVE-2021-4470	TG8 Firewall contains a pre-authentication remote code execution vulnerability in the runphpcmd.php endpoint. The syscmd POST parameter is passed directly to a system command without validation and executed with root privileges. A remote, unauthenticated attacker can supply crafted values to execute arbitrary operating system commands as root, resulting in full device compromise.	N/A	More Details
CVE-2021-4471	TG8 Firewall exposes a directory such as /data/ over HTTP without authentication. This directory stores credential files for previously logged-in users. A remote unauthenticated attacker can enumerate and download files within the directory to obtain valid account usernames and passwords, leading to loss of confidentiality and further unauthorized access.	N/A	More Details
CVE-2022-4985	Vodafone H500s devices running firmware v3.5.10 (hardware model Sercomm VFH500) expose the WiFi access point password via an unauthenticated HTTP endpoint. By sending a crafted GET request to /data/activation.json with specific headers and cookies, a remote attacker can retrieve a JSON document that contains the wifi_password field. This allows an unauthenticated attacker to obtain the WiFi credentials and gain unauthorized access to the wireless network, compromising confidentiality of network traffic and attached systems.	N/A	More Details
CVE-2023-7328	Screen SFT DAB 600/C firmware versions up to and including 1.9.3 contain an improper access control on the user management API allows unauthenticated requests to retrieve structured user data, including account names and connection metadata such as client IP and timeout values.	N/A	More Details
CVE-2025-1256	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-64726	Socket Firewall is an HTTP/HTTPS proxy server that intercepts package manager requests and enforces security policies by blocking dangerous packages. Socket Firewall binary versions (separate from installers) prior to 0.15.5 are vulnerable to arbitrary code execution when run in untrusted project directories. The vulnerability allows an attacker to execute arbitrary code by placing a malicious `.sfw.config` file in a project directory. When a developer runs Socket Firewall commands (e.g., `sfw npm install`) in that directory, the tool loads the `.sfw.config` file and populates environment variables directly into the Node.js process. An attacker can exploit this by setting `NODE_OPTIONS` with a `--require` directive to execute malicious JavaScript code before Socket Firewall's security controls are initialized, effectively bypassing the tool's malicious package detection. The attack vector is indirect and requires a developer to install dependencies for an untrusted project and execute a command within the context of the untrusted project. The vulnerability has been patched in Socket Firewall version 0.15.5. Users should upgrade to version 0.15.5 or later. The fix isolates configuration file values from subprocess environments. Look at `sfw --version` for version information. If users rely on the recommended installation mechanism (e.g. global installation via `npm install -g sfw`) then no workaround is necessary. This wrapper package automatically ensures that users are running the latest version of Socket Firewall. Users who have manually installed the binary and cannot immediately upgrade should avoid running Socket Firewall in untrusted project directories. Before running Socket Firewall in any new project, inspect `.sfw.config` and `.env.local` files for suspicious `NODE_OPTIONS` or other environment variable definitions that reference local files.	N/A	More Details
CVE-2022-4984	ZenTao Biz < 6.5, ZenTao Max < 3.0, ZenTao Open Source Edition < 16.5, and ZenTao Open Source Edition < 16.5.beta1 contain an SQL injection vulnerability in the login functionality. The application does not properly validate the account parameter on /zentao/user-login.html before using it in a database query. A remote unauthenticated attacker can exploit this issue to execute crafted SQL expressions and retrieve sensitive information from the backend database, including user and application data. Exploitation evidence was observed by the Shadowserver Foundation on 2025-02-07 UTC.	N/A	More Details
CVE-2025-12785	Certain HP LaserJet Pro printers may be vulnerable to information disclosure leading to credential exposure by altering the scan/send destination address and/or modifying the LDAP Server.	N/A	More Details
CVE-2025-65064	Rejected reason: Not used	N/A	More Details
CVE-2025-65065	Rejected reason: Not used	N/A	More Details
CVE-2025-65066	Rejected reason: Not used	N/A	More Details

CVE-2025-65067	Rejected reason: Not used	N/A	More Details
CVE-2025-65068	Rejected reason: Not used	N/A	More Details
CVE-2025-40196	In the Linux kernel, the following vulnerability has been resolved: fs: quota: create dedicated workqueue for quota_release_work There is a kernel panic due to WARN_ONCE when panic_on_warn is set. This issue occurs when writeback is triggered due to sync call for an opened file(ie, writeback reason is WB_REASON_SYNC). When f2fs balance is needed at sync path, flush for quota_release_work is triggered. By default quota_release_work is queued to "events_unbound" queue which does not have WQ_MEM_RECLAIM flag. During f2fs balance "writeback" workqueue tries to flush quota_release_work causing kernel panic due to MEM_RECLAIM flag mismatch errors. This patch creates dedicated workqueue with WQ_MEM_RECLAIM flag for work quota_release_work. ------------[cut here]------------ WARNING: CPU: 4 PID: 14867 at kernel/workqueue.c:3721 check_flush_dependency+0x13c/0x148 Call trace: check_flush_dependency+0x13c/0x148 __flush_work+0xd0/0x398 flush_delayed_work+0x44/0x5c dquot_writeback_dquots+0x54/0x318 f2fs_do_quota_sync+0xb8/0x1a8 f2fs_write_checkpoint+0x3cc/0x99c f2fs_gc+0x190/0x750 f2fs_balance_fs+0x110/0x168 f2fs_write_single_data_page+0x474/0x7dc f2fs_write_data_pages+0x7d0/0xd0c do_writepages+0xe0/0x2f4 __writeback_single_inode+0x44/0x4ac writeback_sb_inodes+0x30c/0x538 wb_writeback+0xf4/0x440 wb_workfn+0x128/0x5d4 process_scheduled_works+0x1c4/0x45c worker_thread+0x32c/0x3e8 kthread+0x11c/0x1b0 ret_from_fork+0x10/0x20 Kernel panic - not syncing: kernel: panic_on_warn set ...	N/A	More Details
CVE-2025-40195	In the Linux kernel, the following vulnerability has been resolved: mount: handle NULL values in mnt_ns_release() When calling in listmount() mnt_ns_release() may be passed a NULL pointer. Handle that case gracefully.	N/A	More Details
CVE-2025-40194	In the Linux kernel, the following vulnerability has been resolved: cpufreq: intel_pstate: Fix object lifecycle issue in update_qos_request() The cpufreq_cpu_put() call in update_qos_request() takes place too early because the latter subsequently calls freq_qos_update_request() that indirectly accesses the policy object in question through the QoS request object passed to it. Fortunately, update_qos_request() is called under intel_pstate_driver_lock, so this issue does not matter for changing the intel_pstate operation mode, but it theoretically can cause a crash to occur on CPU device hot removal (which currently can only happen in virt, but it is formally supported nevertheless). Address this issue by modifying update_qos_request() to drop the reference to the policy later.	N/A	More Details
CVE-2025-9316	N-central < 2025.4 can generate sessionIDs for unauthenticated users This issue affects N-central: before 2025.4.	N/A	More Details
CVE-2025-12068	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-11567	CWE-276: Incorrect Default Permissions vulnerability exists that could cause elevated system access when the target installation folder is not properly secured.	N/A	More Details
CVE-2025-11566	CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that would allow an attacker on the local network to gain access to the user account by performing an arbitrary number of authentication attempts with different credentials on the /REST/shutdownnow endpoint.	N/A	More Details
CVE-2025-11565	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause elevated system access when a Web Admin user on the local network tampers with the POST /REST/UpdateJRE request payload.	N/A	More Details
CVE-2025-62876	A Execution with Unnecessary Privileges vulnerability in lightdm-kde-greeter allows escalation from the service user to root.This issue affects lightdm-kde-greeter. before 6.0.4.	N/A	More Details
CVE-2025-12998	Improper Authentication vulnerability in TYPO3 Extension "Modules" codingms/modules.This issue affects Extension "Modules": before 4.3.11, from 5.0.0 before 5.7.4, from 6.0.0 before 6.4.2, from 7.0.0 before 7.5.5.	N/A	More Details
CVE-2025-40177	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Fix bootlog initialization ordering As soon as we queue MHI buffers to receive the bootlog from the device, we could be receiving data. Therefore all the resources needed to process that data need to be setup prior to queuing the buffers. We currently initialize some of the resources after queuing the buffers which creates a race between the probe() and any data that comes back from the device. If the uninitialized resources are accessed, we could see page faults. Fix the init ordering to close the race.	N/A	More Details

CVE-2025-40176	In the Linux kernel, the following vulnerability has been resolved: tls: wait for pending async decryptions if tls_strp_msg_hold fails Async decryption calls tls_strp_msg_hold to create a clone of the input skb to hold references to the memory it uses. If we fail to allocate that clone, proceeding with async decryption can lead to various issues (UAF on the skb, writing into userspace memory after the recv() call has returned). In this case, wait for all pending decryption requests.	N/A	More Details
CVE-2025-40175	In the Linux kernel, the following vulnerability has been resolved: idpf: cleanup remaining SKBs in PTP flows When the driver requests Tx timestamp value, one of the first steps is to clone SKB using skb_get. It increases the reference counter for that SKB to prevent unexpected freeing by another component. However, there may be a case where the index is requested, SKB is assigned and never consumed by PTP flows - for example due to reset during running PTP apps. Add a check in release timestamping function to verify if the SKB assigned to Tx timestamp latch was freed, and release remaining SKBs.	N/A	More Details
CVE-2025-40174	In the Linux kernel, the following vulnerability has been resolved: x86/mm: Fix SMP ordering in switch_mm_irqs_off() Stephen noted that it is possible to not have an smp_mb() between the loaded_mm store and the tlb_gen load in switch_mm(), meaning the ordering against flush_tlb_mm_range() goes out the window, and it becomes possible for switch_mm() to not observe a recent tlb_gen update and fail to flush the TLBs. [dhansen: merge conflict fixed by Ingo]	N/A	More Details
CVE-2025-40173	In the Linux kernel, the following vulnerability has been resolved: net/ip6_tunnel: Prevent perpetual tunnel growth Similarly to ipv4 tunnel, ipv6 version updates dev->needed_headroom, too. While ipv4 tunnel headroom adjustment growth was limited in commit 5ae1e9922bbd ("net: ip_tunnel: prevent perpetual headroom growth"), ipv6 tunnel yet increases the headroom without any ceiling. Reflect ipv4 tunnel headroom adjustment limit on ipv6 version. Credits to Francesco Ruggeri, who was originally debugging this issue and wrote local Arista-specific patch and a reproducer.	N/A	More Details
CVE-2025-40172	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Treat remaining == 0 as error in find_and_map_user_pages() Currently, if find_and_map_user_pages() takes a DMA xfer request from the user with a length field set to 0, or in a rare case, the host receives QAIC_TRANS_DMA_XFER_CONT from the device where resources->xferred_dma_size is equal to the requested transaction size, the function will return 0 before allocating an sgt or setting the fields of the dma_xfer struct. In that case, encode_addr_size_pairs() will try to access the sgt which will lead to a general protection fault. Return an EINVAL in case the user provides a zero-sized ALP, or the device requests continuation after all of the bytes have been transferred.	N/A	More Details
CVE-2025-40171	In the Linux kernel, the following vulnerability has been resolved: nvmet-fc: move lsop put work to nvmet_fc_ls_req_op It’s possible for more than one async command to be in flight from __nvmet_fc_send_ls_req. For each command, a tgtport reference is taken. In the current code, only one put work item is queued at a time, which results in a leaked reference. To fix this, move the work item to the nvmet_fc_ls_req_op struct, which already tracks all resources related to the command.	N/A	More Details
CVE-2025-40170	In the Linux kernel, the following vulnerability has been resolved: net: use dst_dev_rcu() in sk_setup_caps() Use RCU to protect accesses to dst->dev from sk_setup_caps() and sk_dst_gso_max_size(). Also use dst_dev_rcu() in ip6_dst_mtu_maybe_forward(), and ip_dst_mtu_maybe_forward(). ip4_dst_hoplimit() can use dst_dev_net_rcu().	N/A	More Details
CVE-2025-40169	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject negative offsets for ALU ops When verifying BPF programs, the check_alu_op() function validates instructions with ALU operations. The 'offset' field in these instructions is a signed 16-bit integer. The existing check 'insn->off > 1' was intended to ensure the offset is either 0, or 1 for BPF_MOD/BPF_DIV. However, because 'insn->off' is signed, this check incorrectly accepts all negative values (e.g., -1). This commit tightens the validation by changing the condition to '(insn->off != 0 && insn->off != 1)'. This ensures that any value other than the explicitly permitted 0 and 1 is rejected, hardening the verifier against malformed BPF programs.	N/A	More Details
CVE-2025-40168	In the Linux kernel, the following vulnerability has been resolved: smc: Use __sk_dst_get() and dst_dev_rcu() in smc_clc_prfx_match(). smc_clc_prfx_match() is called from smc_listen_work() and not under RCU nor RTNL. Using sk_dst_get(sk)->dev could trigger UAF. Let's use __sk_dst_get() and dst_dev_rcu(). Note that the returned value of smc_clc_prfx_match() is not used in the caller.	N/A	More Details
CVE-2025-40167	In the Linux kernel, the following vulnerability has been resolved: ext4: detect invalid INLINE_DATA + EXTENTS flag combination syzbot reported a BUG_ON in ext4_es_cache_extent() when opening a verity file on a corrupted ext4 filesystem mounted without a journal. The issue is that the filesystem has an inode with both the INLINE_DATA and EXTENTS flags set: EXT4-fs error (device loop0): ext4_cache_extents:545: inode #15: comm syz.0.17: corrupted extent tree: lblk 0 < prev 66 Investigation revealed that the inode has both flags set: DEBUG: inode 15 - flag=1, i_inline_off=164, has_inline=1, extents_flag=1 This is an invalid combination since an inode should have either: - INLINE_DATA: data stored directly in the inode - EXTENTS: data stored in extent-mapped blocks Having both flags causes ext4_has_inline_data() to return true, skipping extent tree validation in __ext4_iget(). The unvalidated out-of-order extents then trigger a BUG_ON in ext4_es_cache_extent() due to integer underflow when calculating hole sizes. Fix this by detecting this invalid flag combination early in ext4_iget() and rejecting the corrupted inode.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Check GuC running state		

CVE-2025-40166	before deregistering exec queue In normal operation, a registered exec queue is disabled and deregistered through the GuC, and freed only after the GuC confirms completion. However, if the driver is forced to unbind while the exec queue is still running, the user may call exec_destroy() after the GuC has already been stopped and CT communication disabled. In this case, the driver cannot receive a response from the GuC, preventing proper cleanup of exec queue resources. Fix this by directly releasing the resources when GuC is not running. Here is the failure dmesg log: " [468.089581] ---[end trace 0000000000000000]--- [468.089608] pci 0000:03:00.0: [drm] *ERROR* GT0: GUC ID manager unclean (1/65535) [468.090558] pci 0000:03:00.0: [drm] GT0: total 65535 [468.090562] pci 0000:03:00.0: [drm] GT0: used 1 [468.090564] pci 0000:03:00.0: [drm] GT0: range 1..1 (1) [468.092716] ------------[cut here]------------ [468.092719] WARNING: CPU: 14 PID: 4775 at drivers/gpu/drm/xe/xe_ttm_vram_mgr.c:298 ttm_vram_mgr_fini+0xf8/0x130 [xe] " v2: use xe_uc_fw_is_running() instead of xe_guc_ct_enabled(). As CT may go down and come back during VF migration. (cherry picked from commit 9b42321a02c50a12b2beb6ae9469606257fbecea)	N/A	More Details
CVE-2025-40165	In the Linux kernel, the following vulnerability has been resolved: media: nxp: imx8-isi: m2m: Fix streaming cleanup on release If streamon/streamoff calls are imbalanced, such as when exiting an application with Ctrl+C when streaming, the m2m usage_count will never reach zero and the ISI channel won't be freed. Besides from that, if the input line width is more than 2K, it will trigger a WARN_ON(): [59.222120] ------------[cut here]------------ [59.226758] WARNING: drivers/media/platform/nxp/imx8-isi/imx8-isi-hw.c:631 at mxc_isi_channel_chain+0xa4/0x120, CPU#4: v4l2-ctl/654 [59.238569] Modules linked in: ap1302 [59.242231] CPU: 4 UID: 0 PID: 654 Comm: v4l2-ctl Not tainted 6.16.0-rc4-next-20250704-06511-gff0e002d480a-dirty #258 PREEMPT [59.253597] Hardware name: NXP i.MX95 15X15 board (DT) [59.258720] pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [59.265669] pc : mxc_isi_channel_chain+0xa4/0x120 [59.270358] lr : mxc_isi_channel_chain+0x44/0x120 [59.275047] sp : ffff8000848c3b40 [59.278348] x29: ffff8000848c3b40 x28: ffff0000859b4c98 x27: ffff800081939f00 [59.285472] x26: 000000000000000a x25: ffff0000859b4cb8 x24: 0000000000000001 [59.292597] x23: ffff0000816f4760 x22: ffff0000816f4258 x21: ffff000084ceb780 [59.299720] x20: ffff000084342ff8 x19: ffff000084340000 x18: 0000000000000000 [59.306845] x17: 0000000000000000 x16: 0000000000000000 x15: 0000ffffdb369e1c [59.313969] x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 [59.321093] x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 [59.328217] x8 : ffff8000848c3d48 x7 : ffff800081930b30 x6 : ffff800081930b30 [59.335340] x5 : ffff0000859b6000 x4 : ffff80008193ae80 x3 : ffff800081022420 [59.342464] x2 : ffff0000852f6900 x1 : 0000000000000001 x0 : ffff000084341000 [59.349590] Call trace: [59.352025] mxc_isi_channel_chain+0xa4/0x120 (P) [59.356722] mxc_isi_m2m_streamon+0x160/0x20c [59.361072] v4l_streamon+0x24/0x30 [59.364556] __video_do_ioctl+0x40c/0x4a0 [59.368560] video_usercopy+0x2bc/0x690 [59.372382] video_ioctl2+0x18/0x24 [59.375857] v4l2_ioctl+0x40/0x60 [59.379168] __arm64_sys_ioctl+0xac/0x104 [59.383172] invoke_syscall+0x48/0x104 [59.386916] el0_svc_common.constprop.0+0xc0/0xe0 [59.391613] do_el0_svc+0x1c/0x28 [59.394915] el0_svc+0x34/0xf4 [59.397966] el0t_64_sync_handler+0xa0/0xe4 [59.402143] el0t_64_sync+0x198/0x19c [59.405801] ---[end trace 0000000000000000]--- Address this issue by moving the streaming preparation and cleanup to the vb2 .prepare_streaming() and .unprepare_streaming() operations. This also simplifies the driver by allowing direct usage of the v4l2_m2m_ioctl_streamon() and v4l2_m2m_ioctl_streamoff() helpers.	N/A	More Details
CVE-2025-40164	In the Linux kernel, the following vulnerability has been resolved: usbnet: Fix using smp_processor_id() in preemptible code warnings Syzbot reported the following warning: BUG: using smp_processor_id() in preemptible [00000000] code: dhcpcd/2879 caller is usbnet_skb_return+0x74/0x490 drivers/net/usb/usbnet.c:331 CPU: 1 UID: 0 PID: 2879 Comm: dhcpcd Not tainted 6.15.0-rc4-syzkaller-00098-g615dca38c2ea #0 PREEMPT(voluntary) Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x16c/0x1f0 lib/dump_stack.c:120 check_preemption_disabled+0xd0/0xe0 lib/smp_processor_id.c:49 usbnet_skb_return+0x74/0x490 drivers/net/usb/usbnet.c:331 usbnet_resume_rx+0x4b/0x170 drivers/net/usb/usbnet.c:708 usbnet_change_mtu+0x1be/0x220 drivers/net/usb/usbnet.c:417 __dev_set_mtu net/core/dev.c:9443 [inline] netif_set_mtu_ext+0x369/0x5c0 net/core/dev.c:9496 netif_set_mtu+0xb0/0x160 net/core/dev.c:9520 dev_set_mtu+0xae/0x170 net/core/dev_api.c:247 dev_ifsioc+0xa31/0x18d0 net/core/dev_ioctl.c:572 dev_ioctl+0x223/0x10e0 net/core/dev_ioctl.c:821 sock_do_ioctl+0x19d/0x280 net/socket.c:1204 sock_ioctl+0x42f/0x6a0 net/socket.c:1311 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:906 [inline] __se_sys_ioctl fs/ioctl.c:892 [inline] __x64_sys_ioctl+0x190/0x200 fs/ioctl.c:892 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x260 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f For historical and portability reasons, the netif_rx() is usually run in the softirq or interrupt context, this commit therefore add local_bh_disable/enable() protection in the usbnet_resume_rx().	N/A	More Details
CVE-2025-40163	In the Linux kernel, the following vulnerability has been resolved: sched/deadline: Stop dl_server before CPU goes offline IBM CI tool reported kernel warning[1] when running a CPU removal operation through drmgr[2]. i.e "drmgr -c cpu -r -q 1" WARNING: CPU: 0 PID: 0 at kernel/sched/cpudeadline.c:219 cpudl_set+0x58/0x170 NIP [c0000000002b6ed8] cpudl_set+0x58/0x170 LR [c0000000002b7cb8] dl_server_timer+0x168/0x2a0 Call Trace: [c000000002c2f8c0] init_stack+0x78c0/0x8000 (unreliable) [c0000000002b7cb8] dl_server_timer+0x168/0x2a0 [c00000000034df84] __hrtimer_run_queues+0x1a4/0x390 [c00000000034f624] hrtimer_interrupt+0x124/0x300 [c00000000002a230] timer_interrupt+0x140/0x320 Git bisects to: commit 4ae8d9aa9f9d ("sched/deadline: Fix dl_server getting stuck") This happens since: - dl_server hrtimer gets enqueued close to cpu offline, when kthread_park enqueues a fair task. - CPU goes offline and drmgr removes it from cpu_present_mask. - hrtimer fires and warning is hit. Fix it by stopping the dl_server before CPU is marked dead. [1]: https://lore.kernel.org/all/8218e149-7718-4432-9312-	N/A	More Details

	f97297c352b9@linux.ibm.com/ [2]: https://github.com/ibm-power-utilities/powerpc-utils/tree/next/src/drmgr [sshegde: wrote the changelog and tested it]		
CVE-2025-40162	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd/sdw_utils: avoid NULL deref when devm_kasprintf() fails devm_kasprintf() may return NULL on memory allocation failure, but the debug message prints cpus->dai_name before checking it. Move the dev_dbg() call after the NULL check to prevent potential NULL pointer dereference.	N/A	More Details
CVE-2025-40161	In the Linux kernel, the following vulnerability has been resolved: mailbox: zynqmp-ipi: Fix SGI cleanup on unbind The driver incorrectly determines SGI vs SPI interrupts by checking IRQ number < 16, which fails with dynamic IRQ allocation. During unbind, this causes improper SGI cleanup leading to kernel crash. Add explicit irq_type field to pdata for reliable identification of SGI interrupts (type-2) and only clean up SGI resources when appropriate.	N/A	More Details
CVE-2025-40160	In the Linux kernel, the following vulnerability has been resolved: xen/events: Return -EEXIST for bound VIRQs Change find_virq() to return -EEXIST when a VIRQ is bound to a different CPU than the one passed in. With that, remove the BUG_ON() from bind_virq_to_irq() to propogate the error upwards. Some VIRQs are per-cpu, but others are per-domain or global. Those must be bound to CPU0 and can then migrate elsewhere. The lookup for per-domain and global will probably fail when migrated off CPU 0, especially when the current CPU is tracked. This now returns -EEXIST instead of BUG_ON(). A second call to bind a per-domain or global VIRQ is not expected, but make it non-fatal to avoid trying to look up the irq, since we don't know which per_cpu(virq_to_irq) it will be in.	N/A	More Details
CVE-2025-40159	In the Linux kernel, the following vulnerability has been resolved: xsk: Harden userspace-supplied xdp_desc validation Turned out certain clearly invalid values passed in xdp_desc from userspace can pass xp_{,un}aligned_validate_desc() and then lead to UBs or just invalid frames to be queued for xmit. desc->len close to ``U32_MAX`` with a non-zero pool->tx_metadata_len can cause positive integer overflow and wraparound, the same way low enough desc->addr with a non-zero pool->tx_metadata_len can cause negative integer overflow. Both scenarios can then pass the validation successfully. This doesn't happen with valid XSk applications, but can be used to perform attacks. Always promote desc->len to ``u64`` first to exclude positive overflows of it. Use explicit check_{add,sub}_overflow() when validating desc->addr (which is ``u64`` already). bloat-o-meter reports a little growth of the code size: add/remove: 0/0 grow/shrink: 2/1 up/down: 60/-16 (44) Function old new delta xskq_cons_peek_desc 299 330 +31 xsk_tx_peek_release_desc_batch 973 1002 +29 xsk_generic_xmit 3148 3132 -16 but hopefully this doesn't hurt the performance much.	N/A	More Details
CVE-2025-40158	In the Linux kernel, the following vulnerability has been resolved: ipv6: use RCU in ip6_output() Use RCU in ip6_output() in order to use dst_dev_rcu() to prevent possible UAF. We can remove rcu_read_lock()/rcu_read_unlock() pairs from ip6_finish_output2().	N/A	More Details
CVE-2025-40157	In the Linux kernel, the following vulnerability has been resolved: EDAC/i10nm: Skip DIMM enumeration on a disabled memory controller When loading the i10nm_edac driver on some Intel Granite Rapids servers, a call trace may appear as follows: UBSAN: shift-out-of-bounds in drivers/edac/skx_common.c:453:16 shift exponent -66 is negative ... __ubsan_handle_shift_out_of_bounds+0x1e3/0x390 skx_get_dimm_info.cold+0x47/0xd40 [skx_edac_common] i10nm_get_dimm_config+0x23e/0x390 [i10nm_edac] skx_register_mci+0x159/0x220 [skx_edac_common] i10nm_init+0xcb0/0x1ff0 [i10nm_edac] ... This occurs because some BIOS may disable a memory controller if there aren't any memory DIMMs populated on this memory controller. The DIMMMTR register of this disabled memory controller contains the invalid value ~0, resulting in the call trace above. Fix this call trace by skipping DIMM enumeration on a disabled memory controller.	N/A	More Details
CVE-2025-40156	In the Linux kernel, the following vulnerability has been resolved: PM / devfreq: mtk-cci: Fix potential error pointer dereference in probe() The drv->sram_reg pointer could be set to ERR_PTR(-EPROBE_DEFER) which would lead to a error pointer dereference. Use IS_ERR_OR_NULL() to check that the pointer is valid.	N/A	More Details
CVE-2025-40155	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: debugfs: Fix legacy mode page table dump logic In legacy mode, SSPTPTR is ignored if TT is not 00b or 01b. SSPTPTR maybe uninitialized or zero in that case and may cause oops like: Oops: general protection fault, probably for non-canonical address 0xf00087d3f000f000: 0000 [#1] SMP NOPTI CPU: 2 UID: 0 PID: 786 Comm: cat Not tainted 6.16.0 #191 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-5.fc42 04/01/2014 RIP: 0010:pgtable_walk_level+0x98/0x150 RSP: 0018:ffffc90000f279c0 EFLAGS: 00010206 RAX: 0000000040000000 RBX: ffffc90000f27ab0 RCX: 000000000000001e RDX: 0000000000000003 RSI: f00087d3f000f000 RDI: f00087d3f0010000 RBP: ffffc90000f27a00 R08: ffffc90000f27a98 R09: 0000000000000002 R10: 0000000000000000 R11: 0000000000000000 R12: f00087d3f000f000 R13: 0000000000000000 R14: 0000000040000000 R15: ffffc90000f27a98 FS: 0000764566dcb740(0000) GS:ffff8881f812c000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000764566d44000 CR3: 0000000109d81003 CR4: 0000000000772ef0 PKRU: 55555554 Call Trace: <TASK> pgtable_walk_level+0x88/0x150 domain_translation_struct_show.isra.0+0x2d9/0x300 dev_domain_translation_struct_show+0x20/0x40 seq_read_iter+0x12d/0x490 ... Avoid walking the page table if TT is not 00b or 01b.	N/A	More Details

CVE-2025-12152	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-61667	The Datadog Agent collects events and metrics from hosts and sends them to Datadog. A vulnerability within the Datadog Linux Host Agent versions 7.65.0 through 7.70.2 exists due to insufficient permissions being set on the `opt/datadog-agent/python-scripts/__pycache__` directory during installation. Code in this directory is only run by the Agent during Agent install/upgrades. This could allow an attacker with local access to modify files in this directory, which would then subsequently be run when the Agent is upgraded, resulting in local privilege escalation. This issue requires local access to the host and a valid low privilege account to be vulnerable. Note that this vulnerability only impacts the Linux Host Agent. Other variations of the Agent including the container, kubernetes, windows host and other agents are not impacted. Version 7.71.0 contains a patch for the issue.	N/A	More Details
CVE-2025-40193	In the Linux kernel, the following vulnerability has been resolved: xtensa: simdisk: add input size check in proc_write_simdisk A malicious user could pass an arbitrarily bad value to memdup_user_nul(), potentially causing kernel crash. This follows the same pattern as commit ee76746387f6 ("netdevsim: prevent bad user input in nsim_dev_health_break_write()")	N/A	More Details
CVE-2025-64099	Open Access Management (OpenAM) is an access management solution. In versions prior to 16.0.0, if the "claims_parameter_supported" parameter is activated, it is possible, thanks to the "oidc-claims-extension.groovy" script, to inject the value of one's choice into a claim contained in the id_token or in the user_info. In the request of an authorize function, a claims parameter containing a JSON file can be injected. This JSON file allows attackers to customize the claims returned by the "id_token" and "user_info" files. This allows for a very wide range of vulnerabilities depending on how clients use claims. For example, if some clients rely on an email field to identify a user, an attacker can choose the email address they want, and therefore assume any identity they choose. Version 16.0.0 fixes the issue.	N/A	More Details
CVE-2025-40192	In the Linux kernel, the following vulnerability has been resolved: Revert "ipmi: fix msg stack when IPMI is disconnected" This reverts commit c608966f3f9c2dca596967501d00753282b395fc. This patch has a subtle bug that can cause the IPMI driver to go into an infinite loop if the BMC misbehaves in a certain way. Apparently certain BMCs do misbehave this way because several reports have come in recently about this.	N/A	More Details
CVE-2025-40191	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix kfd process ref leaking when userptr unmapping kfd_lookup_process_by_pid hold the kfd process reference to ensure it doesn't get destroyed while sending the segfault event to user space. Calling kfd_lookup_process_by_pid as function parameter leaks the kfd process refcount and miss the NULL pointer check if app process is already destroyed.	N/A	More Details
CVE-2025-40190	In the Linux kernel, the following vulnerability has been resolved: ext4: guard against EA inode refcount underflow in xattr update syzkaller found a path where ext4_xattr_inode_update_ref() reads an EA inode refcount that is already <= 0 and then applies ref_change (often -1). That lets the refcount underflow and we proceed with a bogus value, triggering errors like: EXT4-fs error: EA inode <n> ref underflow: ref_count=-1 ref_change=-1 EXT4-fs warning: ea_inode dec ref err=-117 Make the invariant explicit: if the current refcount is non-positive, treat this as on-disk corruption, emit ext4_error_inode(), and fail the operation with -EFSCORRUPTED instead of updating the refcount. Delete the WARN_ONCE() as negative refcounts are now impossible; keep error reporting in ext4_error_inode(). This prevents the underflow and the follow-on orphan/cleanup churn.	N/A	More Details
CVE-2025-40189	In the Linux kernel, the following vulnerability has been resolved: net: usb: lan78xx: Fix lost EEPROM read timeout error(-ETIMEDOUT) in lan78xx_read_raw_eeprom Syzbot reported read of uninitialized variable BUG with following call stack. lan78xx 8-1:1.0 (unnamed net_device) (uninitialized): EEPROM read operation timeout ===== BUG: KMSAN: uninit-value in lan78xx_read_eeprom drivers/net/usb/lan78xx.c:1095 [inline] BUG: KMSAN: uninit-value in lan78xx_init_mac_address drivers/net/usb/lan78xx.c:1937 [inline] BUG: KMSAN: uninit-value in lan78xx_reset+0x999/0x2cd0 drivers/net/usb/lan78xx.c:3241 lan78xx_read_eeprom drivers/net/usb/lan78xx.c:1095 [inline] lan78xx_init_mac_address drivers/net/usb/lan78xx.c:1937 [inline] lan78xx_reset+0x999/0x2cd0 drivers/net/usb/lan78xx.c:3241 lan78xx_bind+0x711/0x1690 drivers/net/usb/lan78xx.c:3766 lan78xx_probe+0x225c/0x3310 drivers/net/usb/lan78xx.c:4707 Local variable sig.i.i created at: lan78xx_read_eeprom drivers/net/usb/lan78xx.c:1092 [inline] lan78xx_init_mac_address drivers/net/usb/lan78xx.c:1937 [inline] lan78xx_reset+0x77e/0x2cd0 drivers/net/usb/lan78xx.c:3241 lan78xx_bind+0x711/0x1690 drivers/net/usb/lan78xx.c:3766 The function lan78xx_read_raw_eeprom failed to properly propagate EEPROM read timeout errors (-ETIMEDOUT). In the fallthrough path, it first attempted to restore the pin configuration for LED outputs and then returned only the status of that restore operation, discarding the original timeout error. As a result, callers could mistakenly treat the data buffer as valid even though the EEPROM read had actually timed out with no data or partial data. To fix this, handle errors in restoring the LED pin configuration separately. If the restore succeeds, return any prior EEPROM timeout error correctly to the caller.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: pwm: berlin: Fix wrong register in suspend/resume The 'enable' register should be BERLIN_PWM_EN rather than BERLIN_PWM_ENABLE,	N/A	More

40188	otherwise, the driver accesses wrong address, there will be cpu exception then kernel panic during suspend/resume.		Details
CVE-2025-40187	In the Linux kernel, the following vulnerability has been resolved: net/sctp: fix a null dereference in sctp_disposition sctp_sf_do_5_1D_ce() If new_asoc->peer.adaptation_ind=0 and sctp_ulpevent_make_authkey=0 and sctp_ulpevent_make_authkey() returns 0, then the variable ai_ev remains zero and the zero will be dereferenced in the sctp_ulpevent_free() function.	N/A	More Details
CVE-2025-40186	In the Linux kernel, the following vulnerability has been resolved: tcp: Don't call reqsk_fastopen_remove() in tcp_conn_request(). syzbot reported the splat below in tcp_conn_request(). [0] If a listener is close()d while a TFO socket is being processed in tcp_conn_request(), inet_csk_reqsk_queue_add() does not set reqsk->sk and calls inet_child_forget(), which calls tcp_disconnect() for the TFO socket. After the cited commit, tcp_disconnect() calls reqsk_fastopen_remove(), where reqsk_put() is called due to !reqsk->sk. Then, reqsk_fastopen_remove() in tcp_conn_request() decrements the last req->rsk_refcnt and frees reqsk, and __reqsk_free() at the drop_and_free label causes the refcount underflow for the listener and double-free of the reqsk. Let's remove reqsk_fastopen_remove() in tcp_conn_request(). Note that other callers make sure tp->fastopen_rsk is not NULL. [0]: refcount_t: underflow; use-after-free. WARNING: CPU: 12 PID: 5563 at lib/refcount.c:28 refcount_warn_saturate (lib/refcount.c:28) Modules linked in: CPU: 12 UID: 0 PID: 5563 Comm: syz-executor Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 07/12/2025 RIP: 0010:refcount_warn_saturate (lib/refcount.c:28) Code: ab e8 8e b4 98 ff 0f 0b c3 cc cc cc cc cc 80 3d a4 e4 d6 01 00 75 9c c6 05 9b e4 d6 01 01 48 c7 c7 e8 df fb ab e8 6a b4 98 ff <0f> 0b e9 03 5b 76 00 cc 80 3d 7d e4 d6 01 00 0f 85 74 ff ff ff c6 RSP: 0018:ffffa79fc0304a98 EFLAGS: 00010246 RAX: d83af4db1c6b3900 RBX: ffff9f65c7a69020 RCX: d83af4db1c6b3900 RDX: 0000000000000000 RSI: 00000000ffff7fff RDI: ffffffffac78a280 RBP: 000000009d781b60 R08: 0000000000007fff R09: ffffffffac6ca280 R10: 0000000000017ffd R11: 0000000000000004 R12: ffff9f65c7b4f100 R13: ffff9f65c7d23c00 R14: ffff9f65c7d26000 R15: ffff9f65c7a64ef8 FS: 00007f9f962176c0(0000) GS:ffff9f65fcf00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000200000000180 CR3: 000000000dbbe006 CR4: 0000000000372ef0 Call Trace: <IRQ> tcp_conn_request (./include/linux/refcount.h:400 ./include/linux/refcount.h:432 ./include/linux/refcount.h:450 ./include/net/sock.h:1965 ./include/net/request_sock.h:131 net/ipv4/tcp_input.c:7301) tcp_rcv_state_process (net/ipv4/tcp_input.c:6708) tcp_v6_do_rcv (net/ipv6/tcp_ipv6.c:1670) tcp_v6_rcv (net/ipv6/tcp_ipv6.c:1906) ip6_protocol_deliver_rcu (net/ipv6/ip6_input.c:438) ip6_input (net/ipv6/ip6_input.c:500) ipv6_rcv (net/ipv6/ip6_input.c:311) __netif_receive_skb (net/core/dev.c:6104) process_backlog (net/core/dev.c:6456) __napi_poll (net/core/dev.c:7506) net_rx_action (net/core/dev.c:7569 net/core/dev.c:7696) handle_softirqs (kernel/softirq.c:579) do_softirq (kernel/softirq.c:480) </IRQ>	N/A	More Details
CVE-2025-40185	In the Linux kernel, the following vulnerability has been resolved: ice: ice_adapter: release xa entry on adapter allocation failure When ice_adapter_new() fails, the reserved XArray entry created by xa_insert() is not released. This causes subsequent insertions at the same index to return -EBUSY, potentially leading to NULL pointer dereferences. Reorder the operations as suggested by Przemek Kitszel: 1. Check if adapter already exists (xa_load) 2. Reserve the XArray slot (xa_reserve) 3. Allocate the adapter (ice_adapter_new) 4. Store the adapter (xa_store)	N/A	More Details
CVE-2025-40184	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Fix debug checking for np-guests using huge mappings When running with transparent huge pages and CONFIG_NVHE_EL2_DEBUG then the debug checking in assert_host_shared_guest() fails on the launch of an np-guest. This WARN_ON() causes a panic and generates the stack below. In __pkvm_host_relax_perms_guest() the debug checking assumes the mapping is a single page but it may be a block map. Update the checking so that the size is not checked and just assumes the correct size. While we're here make the same fix in __pkvm_host_mkyoung_guest(). Info: # lkvm run -k /share/arch/arm64/boot/Image -m 704 -c 8 --name guest-128 Info: Removed ghost socket file "/.lkvm//guest-128.sock". [1406.521757] kvm [141]: nVHE hyp BUG at: arch/arm64/kvm/hyp/nvhe/mem_protect.c:1088! [1406.521804] kvm [141]: nVHE call trace: [1406.521828] kvm [141]: [<ffff8000811676b4>] __kvm_nvhe_hyp_panic+0xb4/0xe8 [1406.521946] kvm [141]: [<ffff80008116d12c>] __kvm_nvhe_assert_host_shared_guest+0xb0/0x10c [1406.522049] kvm [141]: [<ffff80008116f068>] __kvm_nvhe___pkvm_host_relax_perms_guest+0x48/0x104 [1406.522157] kvm [141]: [<ffff800081169df8>] __kvm_nvhe_handle___pkvm_host_relax_perms_guest+0x64/0x7c [1406.522250] kvm [141]: [<ffff800081169f0c>] __kvm_nvhe_handle_trap+0x8c/0x1a8 [1406.522333] kvm [141]: [<ffff8000811680fc>] __kvm_nvhe___skip_pauth_save+0x4/0x4 [1406.522454] kvm [141]: ---[end nVHE call trace]--- [1406.522477] kvm [141]: Hyp Offset: 0xfffece8013600000 [1406.522554] Kernel panic - not syncing: HYP panic: [1406.522554] PS:834003c9 PC:0000b1806db6d170 ESR:00000000f2000800 [1406.522554] FAR:ffff8000804be420 HPFAR:0000000000804be0 PAR:0000000000000000 [1406.522554] VCPU:0000000000000000 [1406.523337] CPU: 3 UID: 0 PID: 141 Comm: kvm-vcpu-0 Not tainted 6.16.0-rc7 #97 PREEMPT [1406.523485] Hardware name: FVP Base RevC (DT) [1406.523566] Call trace: [1406.523629] show_stack+0x18/0x24 (C) [1406.523753] dump_stack_lvl+0xd4/0x108 [1406.523899] dump_stack+0x18/0x24 [1406.524040] panic+0x3d8/0x448 [1406.524184] nvhe_hyp_panic_handler+0x10c/0x23c [1406.524325] kvm_handle_guest_abort+0x68c/0x109c [1406.524500] handle_exit+0x60/0x17c [1406.524630] kvm_arch_vcpu_ioctl_run+0x2e0/0x8c0 [1406.524794] kvm_vcpu_ioctl+0x1a8/0x9cc [1406.524919] __arm64_sys_ioctl+0xac/0x104 [1406.525067] invoke_syscall+0x48/0x10c [1406.525189] el0_svc_common.constprop.0+0x40/0xe0 [1406.525322] do_el0_svc+0x1c/0x28 [1406.525441] el0_svc+0x38/0x120 [1406.525588]	N/A	More Details

	el0t_64_sync_handler+0x10c/0x138 [1406.525750] el0t_64_sync+0x1ac/0x1b0 [1406.525876] SMP: stopping secondary CPUs [1406.525965] Kernel Offset: disabled [1406.526032] CPU features: 0x0000,00000080,8e134ca1,9446773f [1406.526130] Memory Limit: none [1406.959099] ---[end Kernel panic - not syncing: HYP panic: [1406.959099] PS:834003c9 PC:0000b1806db6d170 ESR:00000000f2000800 [1406.959099] FAR:ffff8000804be420 HPFAR:0000000000804be0 PAR:0000000000000000 [1406.959099] VCPU:0000000000000000]		
CVE-2025-34322	Nagios Log Server versions prior to 2026R1.0.1 contain an authenticated command injection vulnerability via the experimental 'Natural Language Queries' feature. Configuration values for this feature are read from the application settings and incorporated into a system command without adequate validation or restriction of special characters. An authenticated user with access to global configuration can abuse these settings to execute arbitrary operating system commands with the privileges of the web server account, leading to compromise of the Log Server host.	N/A	More Details
CVE-2025-34323	Nagios Log Server versions prior to 2026R1.0.1 are vulnerable to local privilege escalation due to unsafe interaction between sudo rules and file system permissions. The web server account is granted passwordless sudo access to certain maintenance scripts while also being a member of a group that has write access to the directory containing those scripts. A local attacker running as the web server user can replace one of the permitted scripts with a malicious program and then execute it via sudo, resulting in arbitrary code execution with root privileges.	N/A	More Details
CVE-2025-40183	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix metadata_dst leak __bpf_redirect_neigh_v{4,6} Cilium has a BPF egress gateway feature which forces outgoing K8s Pod traffic to pass through dedicated egress gateways which then SNAT the traffic in order to interact with stable IPs outside the cluster. The traffic is directed to the gateway via vxlan tunnel in collect md mode. A recent BPF change utilized the bpf_redirect_neigh() helper to forward packets after the arrival and decap on vxlan, which turned out over time that the kmalloc-256 slab usage in kernel was ever-increasing. The issue was that vxlan allocates the metadata_dst object and attaches it through a fake dst entry to the skb. The latter was never released though given bpf_redirect_neigh() was merely setting the new dst entry via skb_dst_set() without dropping an existing one first.	N/A	More Details
CVE-2025-40182	In the Linux kernel, the following vulnerability has been resolved: crypto: skcipher - Fix reqsize handling Commit afddce13ce81d ("crypto: api - Add reqsize to crypto_alg") introduced cra_reqsize field in crypto_alg struct to replace type specific reqsize fields. It looks like this was introduced specifically for ahash and acomp from the commit description as subsequent commits add necessary changes in these alg frameworks. However, this is being recommended for use in all crypto algs [1] instead of setting reqsize using crypto_*_set_reqsize(). Using cra_reqsize in skcipher algorithms, hence, causes memory corruptions and crashes as the underlying functions in the algorithm framework have not been updated to set the reqsize properly from cra_reqsize. [2] Add proper set_reqsize calls in the skcipher init function to properly initialize reqsize for these algorithms in the framework. [1]: https://lore.kernel.org/linux-crypto/aCL8BxpHr5OpT04k@gondor.apana.org.au/ [2]: https://gist.github.com/Pratham-T/24247446f1faf4b7843e4014d5089f6b	N/A	More Details
CVE-2025-64342	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. When the ESP32 is in advertising mode, if it receives a connection request containing an invalid Access Address (AA) of 0x00000000 or 0xFFFFFFFF, advertising may stop unexpectedly. In this case, the controller may incorrectly report a connection event to the host, which can cause the application layer to assume that the device has successfully established a connection. This issue has been fixed in versions 5.5.2, 5.4.3, 5.3.5, 5.2.6, and 5.1.7. At time of publication versions 5.5.2, 5.3.5, and 5.1.7 have not been released but are fixed respectively in commits 3b95b50, e3d7042, and 75967b5.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: x86/kvm: Force legacy PCI hole to UC when overriding MTRRs for TDX/SNP When running as an SNP or TDX guest under KVM, force the legacy PCI hole, i.e. memory between Top of Lower Usable DRAM and 4GiB, to be mapped as UC via a forced variable MTRR range. In most KVM-based setups, legacy devices such as the HPET and TPM are enumerated via ACPI. ACPI enumeration includes a Memory32Fixed entry, and optionally a SystemMemory descriptor for an OperationRegion, e.g. if the device needs to be accessed via a Control Method. If a SystemMemory entry is present, then the kernel's ACPI driver will auto-ioremap the region so that it can be accessed at will. However, the ACPI spec doesn't provide a way to enumerate the memory type of SystemMemory regions, i.e. there's no way to tell software that a region must be mapped as UC vs. WB, etc. As a result, Linux's ACPI driver always maps SystemMemory regions using ioremap_cache(), i.e. as WB on x86. The dedicated device drivers however, e.g. the HPET driver and TPM driver, want to map their associated memory as UC or WC, as accessing PCI devices using WB is unsupported. On bare metal and non-CoCO, the conflicting requirements "work" as firmware configures the PCI hole (and other device memory) to be UC in the MTRRs. So even though the ACPI mappings request WB, they are forced to UC- in the kernel's tracking due to the kernel properly handling the MTRR overrides, and thus are compatible with the drivers' requested WC/UC-. With force WB MTRRs on SNP and TDX guests, the ACPI mappings get their requested WB if the ACPI mappings are established before the dedicated driver code attempts to initialize the device. E.g. if acpi_init() runs before the corresponding device driver is probed, ACPI's WB mapping will "win", and result in the driver's ioremap() failing because the existing WB mapping isn't compatible with the requested WC/UC-. E.g. when a TPM is emulated by the hypervisor (ignoring the security implications of relying on what is allegedly an untrusted		More

2025-40181	entity to store measurements), the TPM driver will request UC and fail: [1.730459] ioremap error for 0xfed40000-0xfed45000, requested 0x2, got 0x0 [1.732780] tpm_tis MSFT0101:00: probe with driver tpm_tis failed with error -12 Note, the '0x2' and '0x0' values refer to "enum page_cache_mode", not x86's memtypes (which frustratingly are an almost pure inversion; 2 == WB, 0 == UC). E.g. tracing mapping requests for TPM TIS yields: Mapping TPM TIS with req_type = 0 WARNING: CPU: 22 PID: 1 at arch/x86/mm/pat/memtype.c:530 memtype_reserve+0x2ab/0x460 Modules linked in: CPU: 22 UID: 0 PID: 1 Comm: swapper/0 Tainted: G W 6.16.0-rc7+ #2 VOLUNTARY Tainted: [W]=WARN Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/29/2025 RIP: 0010:memtype_reserve+0x2ab/0x460 __ioremap_caller+0x16d/0x3d0 ioremap_cache+0x17/0x30 x86_acpi_os_ioremap+0xe/0x20 acpi_os_map_iomem+0x1f3/0x240 acpi_os_map_memory+0xe/0x20 acpi_ex_system_memory_space_handler+0x273/0x440 acpi_ev_address_space_dispatch+0x176/0x4c0 acpi_ex_access_region+0x2ad/0x530 acpi_ex_field_datum_io+0xa2/0x4f0 acpi_ex_extract_from_field+0x296/0x3e0 acpi_ex_read_data_from_field+0xd1/0x460 acpi_ex_resolve_node_to_value+0x2ee/0x530 acpi_ex_resolve_to_value+0x1f2/0x540 acpi_ds_evaluate_name_path+0x11b/0x190 acpi_ds_exec_end_op+0x456/0x960 acpi_ps_parse_loop+0x27a/0xa50 acpi_ps_parse_aml+0x226/0x600 acpi_ps_execute_method+0x172/0x3e0 acpi_ns_evaluate+0x175/0x5f0 acpi_evaluate_object+0x213/0x490 acpi_evaluate_integer+0x6d/0x140 acpi_bus_get_status+0x93/0x150 acpi_add_single_object+0x43a/0x7c0 acpi_bus_check_add+0x149/0x3a0 acpi_bus_check_add_1+0x16/0x30 acpi_ns_walk_namespace+0x22c/0x360 acpi_walk_namespace+0x15c/0x170 acpi_bus_scan+0x1dd/0x200 acpi_scan_init+0xe5/0x2b0 acpi_init+0x264/0x5b0 do_one_i ---truncated---	N/A	Details
CVE-2025-40180	In the Linux kernel, the following vulnerability has been resolved: mailbox: zynqmp-ipi: Fix out-of-bounds access in mailbox cleanup loop The cleanup loop was starting at the wrong array index, causing out-of-bounds access. Start the loop at the correct index for zero-indexed arrays to prevent accessing memory beyond the allocated array bounds.	N/A	More Details
CVE-2025-40179	In the Linux kernel, the following vulnerability has been resolved: ext4: verify orphan file size is not too big In principle orphan file can be arbitrarily large. However orphan replay needs to traverse it all and we also pin all its buffers in memory. Thus filesystems with absurdly large orphan files can lead to big amounts of memory consumed. Limit orphan file size to a sane value and also use kvmalloc() for allocating array of block descriptor structures to avoid large order allocations for sane but large orphan files.	N/A	More Details
CVE-2025-40178	In the Linux kernel, the following vulnerability has been resolved: pid: Add a judgment for ns null in pid_nr_ns __task_pid_nr_ns ns = task_active_pid_ns(current); pid_nr_ns(rcu_dereference(*task_pid_ptr(task, type)), ns); if (pid && ns->level <= pid->level) { Sometimes null is returned for task_active_pid_ns. Then it will trigger kernel panic in pid_nr_ns. For example: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000058 Mem abort info: ESR = 0x0000000096000007 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x07: level 3 translation fault Data abort info: ISV = 0, ISS = 0x00000007, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 39-bit VAs, pgdp=00000002175aa000 [0000000000000058] pgd=08000002175ab003, p4d=08000002175ab003, pud=08000002175ab003, pmd=08000002175be003, pte=0000000000000000 pstate: 834000c5 (Nzcv daIF +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : __task_pid_nr_ns+0x74/0xd0 lr : __task_pid_nr_ns+0x24/0xd0 sp : ffffffc08001bd10 x29: ffffffc08001bd10 x28: ffffffd4422b2000 x27: 0000000000000001 x26: ffffffd442821168 x25: ffffffd442821000 x24: 00000f89492eab31 x23: 00000000000000c0 x22: ffffff806f5693c0 x21: ffffff806f5693c0 x20: 0000000000000001 x19: 0000000000000000 x18: 0000000000000000 x17: 00000000529c6ef0 x16: 00000000529c6ef0 x15: 00000000023a1adc x14: 0000000000000003 x13: 00000000007ef6d8 x12: 001167c391c78800 x11: 00ffffffffffffff x10: 0000000000000000 x9 : 0000000000000001 x8 : ffffff80816fa3c0 x7 : 0000000000000000 x6 : 49534d702d535449 x5 : ffffffc080c4c2c0 x4 : ffffffd43ee128c8 x3 : ffffffd43ee124dc x2 : 0000000000000000 x1 : 0000000000000001 x0 : ffffff806f5693c0 Call trace: __task_pid_nr_ns+0x74/0xd0 ... __handle_irq_event_percpu+0xd4/0x284 handle_irq_event+0x48/0xb0 handle_fasteoi_irq+0x160/0x2d8 generic_handle_domain_irq+0x44/0x60 gic_handle_irq+0x4c/0x114 call_on_irq_stack+0x3c/0x74 do_interrupt_handler+0x4c/0x84 el1_interrupt+0x34/0x58 el1h_64_irq_handler+0x18/0x24 el1h_64_irq+0x68/0x6c account_kernel_stack+0x60/0x144 exit_task_stack_account+0x1c/0x80 do_exit+0x7e4/0xaf8 ... get_signal+0x7bc/0x8d8 do_notify_resume+0x128/0x828 el0_svc+0x6c/0x70 el0t_64_sync_handler+0x68/0xbc el0t_64_sync+0x1a8/0x1ac Code: 35fffe54 911a02a8 f9400108 b4000128 (b9405a69) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception in interrupt	N/A	More Details
CVE-2025-12149	In Search Guard FLX versions 3.1.2 and earlier, while Document-Level Security (DLS) is correctly enforced elsewhere, when the search is triggered from a Signals watch, the DLS rule is not enforced, allowing access to all documents in the queried indices.	N/A	More Details
CVE-2023-7327	Ozeki SMS Gateway versions up to and including 10.3.208 contain a path traversal vulnerability. Successful exploitation allows an unauthenticated attacker to use URL-encoded traversal sequences to read arbitrary files from the underlying filesystem with the privileges of the gateway service, leading to disclosure of sensitive information.	N/A	More Details
CVE-	The Epson Stylus SX510W embedded web management service fails to properly handle consecutive ampersand characters in query parameters when accessing /PRESENTATION/HTML/TOP/INDEX.HTML. A		More

2023-7326	remote attacker can send a malformed request that triggers improper input parsing or memory handling, resulting in the printer process shutting down or powering off, causing a denial of service condition.	N/A	Details
CVE-2025-13216	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-4983	TEC-IT TBarCode version 11.15 contains a vulnerability in the TBarCode11.ocx ActiveX/OCX control's licensing handling (INI-file based) that can be abused to cause remote creation of files on the host filesystem. Depending on where files can be created and which filenames are allowed, this can allow attackers to write files that lead to code execution or persistence under the context of the hosting process.	N/A	More Details
CVE-2022-4982	DBLTek GoIP-1 firmware versions up to and including GHSFVT-1.1-67-5 contain a local file inclusion vulnerability. The device's web server exposes handlers (`frame.html` and `frame.A100.html`) that accept a path parameter (`content` or `sidebar`) which is not properly validated or canonicalized. An attacker can supply directory-traversal sequences to cause the server to read and return arbitrary filesystem files that the webserver user can access. Other GoIP models and firmware versions are likely affected. Exploitation evidence was observed by the Shadowserver Foundation on 2024-03-21 UTC.	N/A	More Details
CVE-2021-4464	FiberHome AN5506-04-FA firmware versions up to and including RP2631 and HG6245D prior to RP2602 contain a stack-based buffer overflow, as the HTTP service ('webs') fails to enforce maximum lengths for Cookie header values. When a cookie longer than 511 bytes is processed, a stack buffer is overrun, leading to a crash or potential control of execution flow.	N/A	More Details
CVE-2021-4463	Longjing Technology BEMS API versions up to and including 1.21 contains an unauthenticated arbitrary file download vulnerability in the 'downloads' endpoint. The 'fileName' parameter is not properly sanitized, allowing attackers to craft traversal sequences and access sensitive files outside the intended directory.	N/A	More Details
CVE-2017-20211	UCanCode E-XD++ Visualization Enterprise Suite contains an untrusted pointer dereference vulnerability via the TKDRAWCAD.TKDrawCADCtrl.1 ActiveX control. This is because it exposes a RotateShape method that dereferences a user-supplied pointer without sufficient validation. A crafted input may cause the control to dereference an attacker-controlled pointer, enabling remote code execution in the context of the hosting process. The vulnerability requires user interaction (instantiation of the ActiveX control via a web page or a file).	N/A	More Details
CVE-2016-15055	JVC VN-T IP-camera models firmware versions up to 2016-08-22 (confirmed on the VN-T216VPRU model) contain a directory traversal vulnerability in the checkcgi endpoint that accepts a user-controlled file parameter. An unauthenticated remote attacker can leverage this vulnerability to read arbitrary files on the device.	N/A	More Details
CVE-2011-10034	AUTOMGEN versions up to and including 8.0.0.7 (also referenced as 8.022) contain a vulnerability in that project file handling frees an object and subsequently dereferences the stale pointer when processing certain malformed fields. The dangling-pointer use enables an attacker to influence an indirect call through attacker-controlled memory, resulting in denial-of-service. In some conditions, remote code execution may be possible.	N/A	More Details
CVE-2023-7329	Tinycontrol LAN Controller v3 (LK3) firmware versions up to 1.58a (hardware v3.8) contain a missing authentication vulnerability in the stm.cgi endpoint. A remote, unauthenticated attacker can send crafted requests to forcibly reboot the device or restore factory settings, leading to a denial of service and configuration loss.	N/A	More Details