SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 August 2025

Generated on 27 August 2025

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-48148	Unrestricted Upload of File with Dangerous Type vulnerability in StoreKeeper B.V. StoreKeeper for WooCommerce allows Using Malicious Files. This issue affects StoreKeeper for WooCommerce: from n/a through 14.4.4.	10.0	More Details
CVE-2025-53577	Improper Control of Generation of Code ('Code Injection') vulnerability in thehp Global DNS allows Remote Code Inclusion. This issue affects Global DNS: from n/a through 3.1.0.	10.0	More Details
CVE-2022-31491	Voltronic Power ViewPower through 1.04-24215, ViewPower Pro through 2.0-22165, and PowerShield Netguard before 1.04-23292 allows a remote attacker to run arbitrary code via an unspecified web interface related to detection of a managed UPS shutting down. An unauthenticated attacker can use this to run arbitrary code immediately regardless of any managed UPS state or presence.	10.0	More Details
CVE-2025-53251	Unrestricted Upload of File with Dangerous Type vulnerability in An-Themes Pin WP allows Upload a Web Shell to a Web Server.This issue affects Pin WP: from n/a before 7.2.	9.9	More Details
CVE-2025-54049	Incorrect Privilege Assignment vulnerability in miniOrange Custom API for WP allows Privilege Escalation. This issue affects Custom API for WP: from n/a through 4.2.2.	9.9	More Details
CVE-2025-48169	Improper Control of Generation of Code ('Code Injection') vulnerability in Jordy Meow Code Engine allows Remote Code Inclusion. This issue affects Code Engine: from n/a through 0.3.3.	9.9	More Details
CVE-2025-53213	Unrestricted Upload of File with Dangerous Type vulnerability in ELEXtensions ReachShip WooCommerce Multi-Carrier & Conditional Shipping allows Using Malicious Files. This issue affects ReachShip WooCommerce Multi-Carrier & Conditional Shipping: from n/a through 4.3.1.	9.9	More Details
CVE-2025-53118	An authentication bypass vulnerability exists which allows an unauthenticated attacker to control administrator backup functions, leading to compromise of passwords, secrets, and application session tokens stored by the Unified PAM.	9.8	More Details
CVE-2025-56214	phpgurukul Hospital Management System 4.0 is vulnerable to SQL Injection in index.php via the username parameter.	9.8	More Details
CVE-2025-53557	A heap-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-53518	An integer overflow vulnerability exists in the ABF parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted ABF file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-53511	A heap-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-52581	An integer overflow vulnerability exists in the GDF parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted GDF file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-48005	A heap-based buffer overflow vulnerability exists in the RHS2000 parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted RHS2000 file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
	An issue in System PDV v1.0 allows a remote attacker to obtain sensitive information via the hash parameter in a URL. The		

CVE-2025-45968	application contains an Insecure Direct Object Reference (IDOR) vulnerability, which occurs due to a lack of proper authorization checks when accessing objects referenced by this parameter. This allows direct access to other users' data or internal resources without proper permission. Successful exploitation of this flaw may result in the exposure of sensitive information.	9.8	More Details
CVE-2025-29515	Incorrect access control in the DELT_file.xgi endpoint of D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 allows attackers to modify arbitrary settings within the device's XML database, including the administrator’s password.	9.8	More Details
CVE-2025-29514	Incorrect access control in the config.xgi function of D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 allows attackers to download the configuration file via providing a crafted web request.	9.8	More Details
CVE-2025-36157	IBM Jazz Foundation 7.0.2 to 7.0.2 iFix035, 7.0.3 to 7.0.3 iFix018, and 7.1.0 to 7.1.0 iFix004 could allow an unauthenticated remote attacker to update server property files that would allow them to perform unauthorized actions.	9.8	More Details
CVE-2025-5821	The Case Theme User plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.3. This is due to the plugin not properly logging a user in with the data that was previously verified through the facebook_ajax_login_callback(). This makes it possible for unauthenticated attackers to log in as administrative users, as long as they have an existing account on the site, and access to the administrative user's email.	9.8	More Details
CVE-2025-7642	The Simpler Checkout plugin for WordPress is vulnerable to Authentication Bypass in versions 0.7.0 to 1.1.9. This is due to the plugin not properly verifying a user's identity prior to logging them in as an admin through the simplerwc_woocommerce_order_created() function. This makes it possible for unauthenticated attackers to log in as other users based on their order ID, which can be an administrator if a site admin has placed a test order.	9.8	More Details
CVE-2022-43110	Voltronic Power ViewPower through 1.04-21353 and PowerShield Netguard before 1.04-23292 allows a remote attacker to configure the system via an unspecified web interface. An unauthenticated remote attacker can make changes to the system including: changing the web interface admin password, view/change system configuration, enumerate connected UPS devices and shut down connected UPS devices. This extends to being able to configure operating system commands that should run if the system detects a connected UPS shutting down.	9.8	More Details
CVE-2025-50722	Insecure Permissions vulnerability in sparkshop v.1.1.7 allows a remote attacker to execute arbitrary code via the Common.php component	9.8	More Details
CVE-2025-51092	The LogIn-SignUp project by VishnuSivadasVS is vulnerable to SQL Injection due to unsafe construction of SQL queries in DataBase.php. The functions logIn() and signUp() build queries by directly concatenating user input and unvalidated table names without using prepared statements. While a prepareData() function exists, it is insufficient to prevent SQL injection and does not sanitize the table name.	9.8	More Details
CVE-2022-45134	Mahara 21.10 before 21.10.6, 22.04 before 22.04.4, and 22.10 before 22.10.1 deserializes user input unsafely during skin import. A particularly structured XML file could cause code execution when being processed.	9.8	More Details
CVE-2025-55613	Tenda O3V2 1.0.0.12(3880) is vulnerable to Buffer Overflow in the fromSafeSetMacFilter function via the mac parameter.	9.8	More Details
CVE-2025-53853	A heap-based buffer overflow vulnerability exists in the ISHNE parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted ISHNE ECG annotations file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-54462	A heap-based buffer overflow vulnerability exists in the Nex parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted .nex file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2025-54480	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8719 of biosig.c on the current master branch (35a819fa), when the Tag is 0: if (tag==0) { if (len!=1) fprintf(stderr,"Warning MFER tag0 incorrect length %i!=1\n",len); curPos += ifread(buf,1,len,hdr); }	9.8	More Details
CVE-2025-54490	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9090 of biosig.c on the current master branch (35a819fa), when the Tag is 64: else if (tag==64) //0x40 { // preamble char tmp[256]; // [1] curPos += ifread(tmp,1,len,hdr); In this case, the overflowed buffer is the newly-declared `tmp` \[1\] instead of `buf`. While `tmp` is larger than `buf`, having a size of 256 bytes, a stack overflow can still occur in cases where `len` is encoded using multiple octets and is greater than 256.	9.8	More Details
CVE-2025-56212	phpgurukul Hospital Management System 4.0 is vulnerable to SQL Injection in add-doctor.php via the docname parameter.	9.8	More Details
CVE-2025-55575	SQL Injection vulnerability in SMM Panel 3.1 allowing remote attackers to gain sensitive information via a crafted HTTP request with action=service_detail.	9.8	More Details
CVE-2025-50900	An issue was discovered in getrebuild/rebuild 4.0.4. The affected source code class is com.rebuild.web.RebuildWebInterceptor, and the affected function is preHandle In the filter code, use CodecUtils.urlDecode(request.getRequestURI()) to obtain the URL-decoded request path, and then determine whether the path endsWith /error. If so, execute return true to skip this Interceptor. Else, redirect to /user/login api. Allowing unauthenticated attackers to gain sensitive information or escalated privileges.	9.8	More Details
CVE-2025-54494	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9205 of biosig.c on the current master branch (35a819fa), when the Tag is 133: else if (tag==133) //0x85 { curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2025-54493	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9184 of biosig.c on the current master branch (35a819fa), when the Tag is 131: else if (tag==131) //0x83 { // Patient Age if (len!=7) fprintf(stderr,"Warning MFER tag131 incorrect length %i!=7\n",len); curPos += ifread(buf,1,len,hdr);	9.8	More Details
	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and		

CVE-2025-54492	Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9141 of biosig.c on the current master branch (35a819fa), when the Tag is 67: else if (tag==67) //0x43: Sample skew { int skew=0; // [1] curPos += ifread(&skew, 1, len,hdr); In this case, the address of the newly-defined integer `skew` \[1\] is overflowed instead of `buf`. This means a stack overflow can occur using much smaller values of `len` in this code path.	9.8	More Details
CVE-2025-54491	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 9191 of biosig.c on the current master branch (35a819fa), when the Tag is 65: else if (tag==65) //0x41: patient event { // event table curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2025-54489	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8970 of biosig.c on the current master branch (35a819fa), when the Tag is 63: else if (tag==63) { uint8_t tag2=255, len2=255; count = 0; while ((count<len) && !(FlagInfiniteLength && len2==0 && tag2==0)){ curPos += ifread(&tag2,1,1,hdr); curPos += ifread(&len2,1,1,hdr); if (VERBOSE_LEVEL==9) fprintf(stdout,"MFER: tag=%3i chan=%2i len=%-4i tag2=%3i len2=%3i curPos=%i %li count=%4i\n",tag,chan,len,tag2,len2,curPos,iftell(hdr),(int)count); if (FlagInfiniteLength && len2==0 && tag2==0) break; count += (2+len2); curPos += ifread(&buf,1,len2,hdr); Here, the number of bytes read is not the Data Length decoded from the current frame in the file (`len`) but rather is a new length contained in a single octet read from the same input file (`len2`). Despite this, a stack-based buffer overflow condition can still occur, as the destination buffer is still `buf`, which has a size of only 128 bytes, while `len2` can be as large as 255.	9.8	More Details
CVE-2025-54481	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8744 of biosig.c on the current master branch (35a819fa), when the Tag is 3: else if (tag==3) { // character code char v[17]; // [1] if (len>16) fprintf(stderr,"Warning MFER tag2 incorrect length %i>16\n",len); curPos += ifread(&v,1,len,hdr); v[len] = 0; In this case, the overflowed buffer is the newly-declared `v` \[1\] instead of `buf`. Since `v` is only 17 bytes large, much smaller values of `len` (even those encoded using a single octet) can trigger an overflow in this code path.	9.8	More Details
CVE-2025-54488	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8850 of biosig.c on the current master branch (35a819fa), when the Tag is 13: else if (tag==13) { if (len>8) fprintf(stderr,"Warning MFER tag13 incorrect length %i>8\n",len); curPos += ifread(&buf,1,len,hdr);	9.8	More Details
CVE-2025-54487	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8842 of biosig.c on the current master branch (35a819fa), when the Tag is 12: else if (tag==12) //0x0C { // sampling resolution if (len>6) fprintf(stderr,"Warning MFER tag12 incorrect length %i>6\n",len); val32 = 0; int8_t v8; curPos += ifread(&UnitCode,1,1,hdr); curPos += ifread(&v8,1,1,hdr); curPos += ifread(buf,1,len-2,hdr); In addition to values of `len` greater than 130 triggering a buffer overflow, a value of `len` smaller than 2 will also trigger a buffer overflow due to an integer underflow when computing `len-2` in this code path.	9.8	More Details
CVE-2025-54486	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8824 of biosig.c on the current master branch (35a819fa), when the Tag is 11: else if (tag==11) //0x0B { // Fs if (len>6) fprintf(stderr,"Warning MFER tag11 incorrect length %i>6\n",len); double fval; curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2025-54485	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8785 of biosig.c on the current master branch (35a819fa), when the Tag is 8: else if (tag==8) { if (len>2) fprintf(stderr,"Warning MFER tag8 incorrect length %i>2\n",len); curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2025-54484	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8779 of biosig.c on the current master branch (35a819fa), when the Tag is 6: else if (tag==6) // 0x06 "number of sequences" { // NRec if (len>4) fprintf(stderr,"Warning MFER tag6 incorrect length %i>4\n",len); curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2025-54483	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8759 of biosig.c on the current master branch (35a819fa), when the Tag is 5: else if (tag==5) //0x05: number of channels { uint16_t oldNS=hdr->NS; if (len>4) fprintf(stderr,"Warning MFER tag5 incorrect length %i>4\n",len); curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2024-53499	Jeewms v3.7 was discovered to contain a SQL injection vulnerability via the CgReportController API.	9.8	More Details
CVE-2025-54482	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.This vulnerability manifests on line 8751 of biosig.c on the current master branch (35a819fa), when the Tag is 4: else if (tag==4) { // SPR if (len>4) fprintf(stderr,"Warning MFER tag4 incorrect length %i>4\n",len); curPos += ifread(buf,1,len,hdr);	9.8	More Details
CVE-2024-52786	An authentication bypass vulnerability in anji-plus AJ-Report up to v1.4.2 allows unauthenticated attackers to execute arbitrary code via a crafted URL.	9.8	More Details
CVE-2024-53496	Incorrect access control in the doFilter function of my-site v1.0.2.RELEASE allows attackers to access sensitive components without authentication.	9.8	More Details
CVE-2025-	An issue in Roadcute API v.1 allows a remote attacker to execute arbitrary code via the application exposing a password reset	9.8	More Details

52395	API endpoint that fails to validate the identity of the requester properly		
CVE-2024-50645	MallChat v1.0-SNAPSHOT has an authentication bypass vulnerability. An attacker can exploit this vulnerability to access API without any token.	9.8	More Details
CVE-2025-24285	Multiple Improper Input Validation vulnerabilities in UniFi Connect EV Station Lite may allow a Command Injection by a malicious actor with network access to the UniFi Connect EV Station Lite. Affected Products: UniFi Connect EV Station Lite (Version 1.5.1 and earlier) Mitigation: Update UniFi Connect EV Station Lite to Version 1.5.2 or later	9.8	More Details
CVE-2024-57155	Incorrect access control in radar v1.0.8 allows attackers to bypass authentication and access sensitive APIs without a token.	9.8	More Details
CVE-2025-54988	Critical XXE in Apache Tika (tika-parser-pdf-module) in Apache Tika 1.13 through and including 3.2.1 on all platforms allows an attacker to carry out XML External Entity injection via a crafted XFA file inside of a PDF. An attacker may be able to read sensitive data or trigger malicious requests to internal resources or third-party servers. Note that the tika-parser-pdf-module is used as a dependency in several Tika packages including at least: tika-parsers-standard-modules, tika-parsers-standard-package, tika-app, tika-grpc and tika-server-standard. Users are recommended to upgrade to version 3.2.2, which fixes this issue.	9.8	More Details
CVE-2024-57154	Incorrect access control in dts-shop v0.0.1-SNAPSHOT allows attackers to bypass authentication via sending a crafted payload to /admin/auth/index.	9.8	More Details
CVE-2025-55444	A SQL injection vulnerability exists in the id2 parameter of the cancel_booking.php page in Online Artwork and Fine Arts MCA Project 1.0. A remote attacker can inject arbitrary SQL queries, leading to database enumeration and potential remote code execution.	9.8	More Details
CVE-2025-50904	There is an authentication bypass vulnerability in WinterChenS my-site thru commit 6c79286 (2025-06-11). An attacker can exploit this vulnerability to access /admin/ API without any token.	9.8	More Details
CVE-2025-50901	JeeWMS 771e4f5d0c01ffdeae1671be4cf102b73a3fe644 (2025-05-19) contains incorrect authentication bypass vulnerability, which can lead to arbitrary file reading.	9.8	More Details
CVE-2024-50640	jeewx-boot 1.3 has an authentication bypass vulnerability in the preHandle function	9.8	More Details
CVE-2024-57157	Incorrect access control in Jantent v1.1 allows attackers to bypass authentication and access sensitive APIs without a token.	9.8	More Details
CVE-2025-27129	An authentication bypass vulnerability exists in the HTTP authentication functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted HTTP request can lead to arbitrary code execution. An attacker can send packets to trigger this vulnerability.	9.8	More Details
CVE-2025-54713	Authentication Bypass Using an Alternate Path or Channel vulnerability in magepeopleteam Taxi Booking Manager for WooCommerce allows Authentication Abuse. This issue affects Taxi Booking Manager for WooCommerce: from n/a through 1.3.0.	9.8	More Details
CVE-2025-54014	Deserialization of Untrusted Data vulnerability in QuanticaLabs MediCenter - Health Medical Clinic allows Object Injection. This issue affects MediCenter - Health Medical Clinic: from n/a through 15.1.	9.8	More Details
CVE-2025-53580	Incorrect Privilege Assignment vulnerability in quantumcloud Simple Business Directory Pro allows Privilege Escalation. This issue affects Simple Business Directory Pro: from n/a through n/a.	9.8	More Details
CVE-2025-53299	Deserialization of Untrusted Data vulnerability in ThemeMakers ThemeMakers Visual Content Composer allows Object Injection. This issue affects ThemeMakers Visual Content Composer: from n/a through 1.5.8.	9.8	More Details
CVE-2025-8895	The WP Webhooks plugin for WordPress is vulnerable to arbitrary file copy due to missing validation of user-supplied input in all versions up to, and including, 3.3.5. This makes it possible for unauthenticated attackers to copy arbitrary files on the affected site's server to arbitrary locations. This can be used to copy the contents of wp-config.php into a text file which can then be accessed in a browser to reveal database credentials.	9.8	More Details
CVE-2025-27214	A Missing Authentication for Critical Function vulnerability in the UniFi Connect EV Station Pro may allow a malicious actor with physical or adjacent access to perform an unauthorized factory reset. Affected Products: UniFi Connect EV Station Pro (Version 1.5.18 and earlier) Mitigation: Update UniFi Connect EV Station Pro to Version 1.5.27 or later	9.8	More Details
CVE-2025-52095	An issue in PDQ Smart Deploy V.3.0.2040 allows an attacker to escalate privileges via the Credential encryption routines in SDCommon.dll	9.8	More Details
CVE-2025-9254	WebITR developed by Uniong has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to log into the system as arbitrary users by exploiting a specific functionality.	9.8	More Details
CVE-2025-57105	The DI-7400G+ router has a command injection vulnerability, which allows attackers to execute arbitrary commands on the device. The sub_478D28 function in in mng_platform.asp, and sub_4A12DC function in wayos_ac_server.asp of the jhttpd program, with the parameter ac_mng_srv_host.	9.8	More Details
CVE-2025-55619	Reolink v4.54.0.4.20250526 was discovered to contain a hardcoded encryption key and initialization vector. An attacker can leverage this vulnerability to decrypt access tokens and web session tokens stored inside the app via reverse engineering.	9.8	More Details
CVE-2025-55398	An issue was discovered in mouse07410 asn1c thru 0.9.29 (2025-03-20) - a fork of vlm asn1c. In UPER (Unaligned Packed Encoding Rules), asn1c-generated decoders fail to enforce INTEGER constraints when the bound is positive and exceeds 32 bits in length, potentially allowing incorrect or malicious input to be processed.	9.8	More Details
CVE-2024-50644	zhisheng17 blog 3.0.1-SNAPSHOT has an authentication bypass vulnerability. An attacker can exploit this vulnerability to access API without any token.	9.8	More Details
CVE-2025-29366	In mupen64plus v2.6.0 there is an array overflow vulnerability in the write_rdram_regs and write_rdram_regs functions, which enables executing arbitrary commands on the host machine.	9.8	More Details
CVE-2025-29365	spimsimulator spim v9.1.24 and before is vulnerable to Buffer Overflow in READ_STRING_SYSCALL.	9.8	More Details

CVE-2025-41702	The JWT secret key is embedded in the egOS WebGUI backend and is readable to the default user. An unauthenticated remote attacker can generate valid HS256 tokens and bypass authentication/authorization due to the use of hard-coded cryptographic key.	9.8	More Details
CVE-2025-53763	Improper access control in Azure Databricks allows an unauthorized attacker to elevate privileges over a network.	9.8	More Details
CVE-2025-3128	A remote unauthenticated attacker who has bypassed authentication could execute arbitrary OS commands to disclose, tamper with, destroy or delete information in Mitsubishi Electric smartRTU, or cause a denial-of service condition on the product.	9.8	More Details
CVE-2025-52352	Aikaan IoT management platform v3.25.0325-5-g2e9c59796 provides a configuration to disable user sign-up in distributed deployments by hiding the sign-up option on the login page UI. However, the sign-up API endpoint remains publicly accessible and functional, allowing unauthenticated users to register accounts via APIs even when the feature is disabled. This leads to authentication bypass and unauthorized access to admin portals, violating intended access controls.	9.8	More Details
CVE-2025-57754	eslint-ban-moment is an Eslint plugin for final assignment in VIHU. In 3.0.0 and earlier, a sensitive Supabase URI is exposed in .env. A valid Supabase URI with embedded username and password will allow an attacker complete unauthorized access and control over database and user data. This could lead to data exfiltration, modification or deletion.	9.8	More Details
CVE-2025-4609	Incorrect handle provided in unspecified circumstances in Mojo in Google Chrome on Windows prior to 136.0.7103.113 allowed a remote attacker to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	9.6	More Details
CVE-2025-49381	Cross-Site Request Forgery (CSRF) vulnerability in ads.txt Guru ads.txt Guru Connect allows Cross Site Request Forgery. This issue affects ads.txt Guru Connect: from n/a through 1.1.1.	9.6	More Details
CVE-2025-53120	A path traversal vulnerability in unauthenticated upload functionality allows a malicious actor to upload binaries and scripts to the server’s configuration and web root directories, achieving remote code execution on the Unified PAM server.	9.4	More Details
CVE-2025-55746	Directus is a real-time API and App dashboard for managing SQL database content. From 10.8.0 to before 11.9.3, a vulnerability exists in the file update mechanism which allows an unauthenticated actor to modify existing files with arbitrary contents (without changes being applied to the files' database-resident metadata) and / or upload new files, with arbitrary content and extensions, which won't show up in the Directus UI. This vulnerability is fixed in 11.9.3.	9.3	More Details
CVE-2025-26496	Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in Salesforce Tableau Server, Tableau Desktop on Windows, Linux (File Upload modules) allows Local Code Inclusion.This issue affects Tableau Server, Tableau Desktop: before 2025.1.3, before 2024.2.12, before 2023.3.19.	9.3	More Details
CVE-2025-54726	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Miguel Useche JS Archive List allows SQL Injection. This issue affects JS Archive List: from n/a through n/a.	9.3	More Details
CVE-2025-54048	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in miniOrange Custom API for WP allows SQL Injection. This issue affects Custom API for WP: from n/a through 4.2.2.	9.3	More Details
CVE-2025-53795	Improper authorization in Microsoft PC Manager allows an unauthorized attacker to elevate privileges over a network.	9.1	More Details
CVE-2025-7390	A malicious client can bypass the client certificate trust check of an opc.https server when the server endpoint is configured to allow only secure communication.	9.1	More Details
CVE-2025-54677	Unrestricted Upload of File with Dangerous Type vulnerability in vcita Online Booking & Scheduling Calendar for WordPress by vcita allows Using Malicious Files. This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.5.3.	9.1	More Details
CVE-2025-27217	A Server-Side Request Forgery (SSRF) in the UISP Application may allow a malicious actor with certain permissions to make requests outside of UISP Application scope.	9.1	More Details
CVE-2024-45438	An issue was discovered in TitanHQ SpamTitan Email Security Gateway 8.00.x before 8.00.101 and 8.01.x before 8.01.14. The file quarantine.php within the SpamTitan interface allows unauthenticated users to trigger account-level actions using a crafted GET request. Notably, when a non-existent email address is provided as part of the email parameter, SpamTitan will automatically create a user record and associate quarantine settings with it - all without requiring authentication.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-50503	A vulnerability in the password reset workflow of the Touch Lebanon Mobile App 2.20.2 allows an attacker to bypass the OTP reset password mechanism. By manipulating the reset process, an unauthorized user may be able to reset the password and gain access to the account without needing to provide a legitimate authentication factor, such as an OTP. This compromises account security and allows for potential unauthorized access to user data.	8.8	More Details
CVE-2025-9393	A vulnerability was detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This vulnerability affects the function addStaProfile of the file /goform/addStaProfile. Performing manipulation of the argument profile_name/Ssid/wep_key_1/wep_key_2/wep_key_3/wep_key_4/wep_key_length/wep_default_key/cipher/passphrase results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-52930	A memory corruption vulnerability exists in the BMPv3 RLE Decoding functionality of the SAIL Image Decoding Library v0.9.8. When decompressing the image data from a specially crafted .bmp file, a heap-based buffer overflow can occur which allows for remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-9481	A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function setIpv6 of the file /goform/setIpv6. The manipulation of the argument tunrd_Prefix leads to stack-based buffer overflow. Remote exploitation of the attack is possible. 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.	8.8	More Details

CVE-2025-52351	Aikaan IoT management platform v3.25.0325-5-g2e9c59796 sends a newly generated password to users in plaintext via email and also includes the same password as a query parameter in the account activation URL (e.g., https://domain.com/activate=xyz). This practice can result in password exposure via browser history, proxy logs, referrer headers, and email caching. The vulnerability impacts user credential confidentiality during initial onboarding.	8.8	More Details
CVE-2025-9482	A vulnerability was detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This impacts the function portRangeForwardAdd of the file /goform/portRangeForwardAdd. The manipulation of the argument ruleName/schedule/inboundFilter/TCPPorts/UDPPorts results in stack-based buffer overflow. 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.	8.8	More Details
CVE-2025-9483	A flaw has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected is the function singlePortForwardAdd of the file /goform/singlePortForwardAdd. This manipulation of the argument ruleName/schedule/inboundFilter causes stack-based buffer overflow. 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.	8.8	More Details
CVE-2025-52456	A memory corruption vulnerability exists in the WebP Image Decoding functionality of the SAIL Image Decoding Library v0.9.8. When loading a specially crafted .webp animation an integer overflow can be made to occur when calculating the stride for decoding. Afterwards, this will cause a heap-based buffer to overflow when decoding the image which can lead to remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-49382	Cross-Site Request Forgery (CSRF) vulnerability in DexignZone JobZilla - Job Board WordPress Theme allows Privilege Escalation. This issue affects JobZilla - Job Board WordPress Theme: from n/a through 2.0.	8.8	More Details
CVE-2024-57491	Authentication Bypass vulnerability in jobx up to v1.0.1-RELEASE allows an attacker can exploit this vulnerability to access sensitive API without any token via the preHandle function.	8.8	More Details
CVE-2025-50129	A memory corruption vulnerability exists in the PCX Image Decoding functionality of the SAIL Image Decoding Library v0.9.8. When decoding the image data from a specially crafted .tga file, a heap-based buffer overflow can occur which allows for remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-46407	A memory corruption vulnerability exists in the BMPv3 Palette Decoding functionality of the SAIL Image Decoding Library v0.9.8. When loading a specially crafted .bmp file, an integer overflow can be made to occur which will cause a heap-based buffer to overflow when reading the palette from the image. These conditions can allow for remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-51991	XWiki through version 17.3.0 is vulnerable to Server-Side Template Injection (SSTI) in the Administration interface, specifically within the HTTP Meta Info field of the Global Preferences Presentation section. An authenticated administrator can inject crafted Apache Velocity template code, which is rendered on the server side without proper validation or sandboxing. This enables the execution of arbitrary template logic, which may expose internal server information or, in specific configurations, lead to further exploitation such as remote code execution or sensitive data leakage. The vulnerability resides in improper handling of dynamic template rendering within user-supplied configuration fields.	8.8	More Details
CVE-2025-35984	A memory corruption vulnerability exists in the PCX Image Decoding functionality of the SAIL Image Decoding Library v0.9.8. When decoding the image data from a specially crafted .pcx file, a heap-based buffer overflow can occur which allows for remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-32468	A memory corruption vulnerability exists in the BMPv3 Image Decoding functionality of the SAIL Image Decoding Library v0.9.8. When loading a specially crafted .bmp file, an integer overflow can be made to occur when calculating the stride for decoding. Afterwards, this will cause a heap-based buffer to overflow when decoding the image which can lead to remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-48165	Incorrect Privilege Assignment vulnerability in DELUCKS DELUCKS SEO allows Privilege Escalation. This issue affects DELUCKS SEO: from n/a through 2.6.0.	8.8	More Details
CVE-2025-48164	Incorrect Privilege Assignment vulnerability in Brainstorm Force SureDash allows Privilege Escalation. This issue affects SureDash: from n/a through 1.0.3.	8.8	More Details
CVE-2025-49399	Cross-Site Request Forgery (CSRF) vulnerability in Basix NEX-Forms allows Cross Site Request Forgery. This issue affects NEX-Forms: from n/a through 9.1.3.	8.8	More Details
CVE-2025-53085	A memory corruption vulnerability exists in the PSD RLE Decoding functionality of the SAIL Image Decoding Library v0.9.8. When decompressing the image data from a specially crafted .psd file, a heap-based buffer overflow can occur which allows for remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-55743	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. Before 0.2.1, the image upload at the user creation feature performs only client side file type validation. A user can capture the request by uploading an image, capture the request through a Proxy like Burp suite. Make changes to the file extension and content. The vulnerability is fixed in 0.2.1.	8.8	More Details
CVE-2025-9443	A flaw has been found in Tenda CH22 1.0.0.1. This vulnerability affects the function formeditUserName of the file /goform/editUserName. Executing manipulation of the argument new_account can lead to buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-55368	Incorrect access control in the component \controller\RoleController.java of jshERP v3.5 allows unauthorized attackers to arbitrarily modify the supplier status under any account.	8.8	More Details
CVE-2025-54007	Deserialization of Untrusted Data vulnerability in PickPlugins Post Grid and Gutenberg Blocks allows Object Injection. This issue affects Post Grid and Gutenberg Blocks: from n/a through 2.3.11.	8.8	More Details
CVE-	hippo4j 1.0.0 to 1.5.0, uses a hard-coded secret key in its JWT (JSON Web Token) creation. This allows attackers with access to the source		

2025-51606	code or compiled binary to forge valid access tokens and impersonate any user, including privileged ones such as "admin". The vulnerability poses a critical security risk in systems where authentication and authorization rely on the integrity of JWTs.	8.8	More Details
CVE-2025-9299	A vulnerability has been found in Tenda M3 1.0.0.12. Affected by this vulnerability is the function formGetMasterPassengerAnalyseData of the file /goform/getMasterPassengerAnalyseData. The manipulation of the argument Time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-54735	Incorrect Privilege Assignment vulnerability in Emraan Cheema CubeWP Framework allows Privilege Escalation. This issue affects CubeWP Framework: from n/a through 1.1.24.	8.8	More Details
CVE-2025-5931	The Dokan Pro plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 4.0.5. This is due to the plugin not properly validating a user's identity prior to updating their password during a staff password reset. This makes it possible for authenticated attackers, with vendor-level access and above, to elevate their privilege to the level of a staff member and then change arbitrary user passwords, including those of administrators in order to gain access to their accounts. By default, the plugin allows customers to become vendors.	8.8	More Details
CVE-2025-9298	A flaw has been found in Tenda M3 1.0.0.12. Affected is the function formQuickIndex of the file /goform/QuickIndex. Executing manipulation of the argument PPPOEPassword can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-53510	A memory corruption vulnerability exists in the PSD Image Decoding functionality of the SAIL Image Decoding Library v0.9.8. When loading a specially crafted .psd file, an integer overflow can be made to occur when calculating the stride for decoding. Afterwards, this will cause a heap-based buffer to overflow when decoding the image which can lead to remote code execution. An attacker will need to convince the library to read a file to trigger this vulnerability.	8.8	More Details
CVE-2025-9303	A security flaw has been discovered in TOTOLINK A720R 4.1.5cu.630_B20250509. This issue affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. Performing manipulation of the argument desc results in buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	8.8	More Details
CVE-2025-9297	A vulnerability was detected in Tenda i22 1.0.0.3(4687). This impacts the function formWeixinAuthInfoGet of the file /goform/wxportalauth. Performing manipulation of the argument Type results in stack-based buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-57760	Langflow is a tool for building and deploying AI-powered agents and workflows. A privilege escalation vulnerability exists in Langflow containers where an authenticated user with RCE access can invoke the internal CLI command langflow superuser to create a new administrative user. This results in full superuser access, even if the user initially registered through the UI as a regular (non-admin) account. A patched version has not been made public at this time.	8.8	More Details
CVE-2025-55409	FoxCMS 1.2.6, there is a Cross Site Scripting vulnerability in /index.php/article. This allows attackers to execute arbitrary code.	8.8	More Details
CVE-2025-55420	A Reflected Cross Site Scripting (XSS) vulnerability was found in /index.php in FoxCMS v1.2.6. When a crafted script is sent via a GET request, it is reflected unsanitized into the HTML response. This permits execution of arbitrary JavaScript code when a logged-in user submits the malicious input.	8.8	More Details
CVE-2025-57761	WeGIA is a Web manager for charitable institutions. Prior to 3.4.10, there is a SQL Injection vulnerability in the /html/funcionario/dependente_remover.php endpoint, specifically in the id_funcionario parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. This vulnerability is fixed in 3.4.10.	8.8	More Details
CVE-2025-53560	Deserialization of Untrusted Data vulnerability in rascals Noisa allows Object Injection. This issue affects Noisa: from n/a through 2.6.0.	8.8	More Details
CVE-2025-26467	Privilege Defined With Unsafe Actions vulnerability in Apache Cassandra. An user with MODIFY permission ON ALL KEYSPACES can escalate privileges to superuser within a targeted Cassandra cluster via unsafe actions to a system resource. Operators granting data MODIFY permission on all keyspaces on affected versions should review data access rules for potential breaches. This issue affects Apache Cassandra 3.0.30, 3.11.17, 4.0.16, 4.1.7, 5.0.2, but this advisory is only for 4.0.16 because the fix to CVE-2025-23015 was incorrectly applied to 4.0.16, so that version is still affected. Users in the 4.0 series are recommended to upgrade to version 4.0.17 which fixes the issue. Users from 3.0, 3.11, 4.1 and 5.0 series should follow recommendation from CVE-2025-23015.	8.8	More Details
CVE-2025-9392	A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function qosClassifier of the file /goform/qosClassifier. Such manipulation of the argument dir/sFromPort/sToPort/dFromPort/dToPort/protocol/layer7/dscp/remark_dscp leads to stack-based buffer overflow. 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.	8.8	More Details
CVE-2025-55731	Frappe is a full-stack web application framework. A carefully crafted request could extract data that the user would normally not have access to, via SQL injection. This vulnerability is fixed in 15.74.2 and 14.96.15.	8.8	More Details
CVE-2025-50902	Cross Site Request Forgery (CSRF) vulnerability in old-peanut Open-Shop (aka old-peanut/wechat_applet__open_source) thru 1.0.0 allows attackers to gain sensitive information via crafted HTTP Post message.	8.8	More Details
CVE-2025-9245	A vulnerability was detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This issue affects the function WPSSTAPINEnr of the file /goform/WPSSTAPINEnr. Performing manipulation of the argument ssid results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9246	A flaw has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Impacted is the function check_port_conflict of the file /goform/check_port_conflict. Executing manipulation of the argument single_port_rule/port_range_rule can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about	8.8	More Details

	this disclosure but did not respond in any way.		
CVE-2025-9247	A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. The affected element is the function setVlan of the file /goform/setVlan. The manipulation of the argument vlan_set leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9248	A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. The impacted element is the function RP_pingGatewayByBBS of the file /goform/RP_pingGatewayByBBS. The manipulation of the argument ssidhex results in stack-based buffer overflow. The attack may be performed from a remote location. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9249	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function DHCPReserveAddGroup of the file /goform/DHCPReserveAddGroup. This manipulation of the argument enable_group/name_group/ip_group/mac_group causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9250	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This impacts the function setPWDbyBBS of the file /goform/setPWDbyBBS. Such manipulation of the argument hint leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9251	A security flaw has been discovered in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected is the function sta_wps_pin of the file /goform/sta_wps_pin. Performing manipulation of the argument Ssid results in stack-based buffer overflow. The attack can be initiated 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.	8.8	More Details
CVE-2025-9252	A weakness has been identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected by this vulnerability is the function DisablePasswordAlertRedirect of the file /goform/DisablePasswordAlertRedirect. Executing manipulation of the argument hint can lead to stack-based buffer overflow. The attack can be launched 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.	8.8	More Details
CVE-2025-8145	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.2.4 via deserialization of untrusted input in the get_lead_fields function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in a Contact Form 7 plugin allows attackers to delete arbitrary files. Additionally, in certain server configurations, Remote Code Execution is possible	8.8	More Details
CVE-2025-8141	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_associated_files function in all versions up to, and including, 3.2.4. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.8	More Details
CVE-2025-9253	A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected by this issue is the function RP_doSpecifySiteSurvey of the file /goform/RP_doSpecifySiteSurvey. The manipulation of the argument ssidhex leads to stack-based buffer overflow. The attack may 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.	8.8	More Details
CVE-2025-27216	Multiple Incorrect Permission Assignment for Critical Resource in UISP Application may allow a malicious actor with certain permissions to escalate privileges.	8.8	More Details
CVE-2025-9132	Out of bounds write in V8 in Google Chrome prior to 139.0.7258.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-43300	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.7.8, macOS Ventura 13.7.8, iPadOS 17.7.10, macOS Sequoia 15.6.1, iOS 18.6.2 and iPadOS 18.6.2. Processing a malicious image file may result in memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.	8.8	More Details
CVE-2025-57800	Audiobookshelf is an open-source self-hosted audiobook server. In versions 2.6.0 through 2.26.3, the application does not properly restrict redirect callback URLs during OIDC authentication. An attacker can craft a login link that causes Audiobookshelf to store an arbitrary callback in a cookie, which is later used to redirect the user after authentication. The server then issues a 302 redirect to the attacker-controlled URL, appending sensitive OIDC tokens as query parameters. This allows an attacker to obtain the victim's tokens and perform full account takeover, including creating persistent admin users if the victim is an administrator. Tokens are further leaked via browser history, Referer headers, and server logs. This vulnerability impacts all Audiobookshelf deployments using OIDC; no IdP misconfiguration is required. The issue is fixed in version 2.28.0. No known workarounds exist.	8.8	More Details
CVE-2025-57790	An issue was discovered in Commvault before 11.36.60. A security vulnerability has been identified that allows remote attackers to perform unauthorized file system access through a path traversal issue. The vulnerability may lead to remote code execution.	8.8	More Details
CVE-2025-52085	An SQL injection vulnerability in Yoosee application v6.32.4 allows authenticated users to inject arbitrary SQL queries via a request to a backend API endpoint. Successful exploitation enables extraction of sensitive database information, including but not limited to, the database server banner and version, current database user and schema, the current DBMS user privileges, and arbitrary data from any table.	8.8	More Details
CVE-2025-55573	QuantumNous new-api v.0.8.5.2 is vulnerable to Cross Site Scripting (XSS).	8.8	More Details
CVE-2025-	A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function portTriggerManageRule of the file /goform/portTriggerManageRule. The manipulation of the argument triggerRuleName/schedule leads to stack-based buffer overflow.	8.8	More Details

9363	Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-9361	A vulnerability was detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. The affected element is the function ipRangeBlockManageRule of the file /goform/ipRangeBlockManageRule. Performing manipulation of the argument ipRangeBlockRuleName/scheduleIp/ipRangeBlockRuleIpAddr results in stack-based buffer overflow. The attack may be initiated 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.	8.8	More Details
CVE-2025-9360	A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Impacted is the function accessControlAdd of the file /goform/accessControlAdd. Such manipulation of the argument ruleName/schedule leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9359	A weakness has been identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This issue affects the function RP_checkCredentialsByBBS of the file /goform/RP_checkCredentialsByBBS. This manipulation of the argument ssidhex/pwd causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9358	A security flaw has been discovered in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This vulnerability affects the function setSysAdm of the file /goform/setSysAdm. The manipulation of the argument admpasshint results in stack-based buffer overflow. It is possible to launch 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.	8.8	More Details
CVE-2025-48142	Incorrect Privilege Assignment vulnerability in Saad Iqbal Bookify allows Privilege Escalation. This issue affects Bookify: from n/a through 1.0.9.	8.8	More Details
CVE-2025-52287	OperaMasks SDK ELite Script Engine v0.5.0 was discovered to contain a deserialization vulnerability.	8.8	More Details
CVE-2025-9357	A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This affects the function langSwitchByBBS of the file /goform/langSwitchByBBS. The manipulation of the argument langSelectionOnly leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9356	A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected by this issue is the function inboundFilterAdd of the file /goform/inboundFilterAdd. Executing manipulation of the argument ruleName can lead to stack-based buffer overflow. The attack may be performed from a remote location. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-9355	A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. Affected by this vulnerability is the function scheduleAdd of the file /goform/scheduleAdd. Performing manipulation of the argument ruleName results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-6791	On the monitoring event logs page, it is possible to alter the http request to insert a payload in the DB. Caused by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Centreon web (Monitoring event logs modules) allows SQL Injection. This issue affects web: from 24.10.0 before 24.10.9, from 24.04.0 before 24.04.16, from 23.10.0 before 23.10.26.	8.8	More Details
CVE-2025-6366	The Event List plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 2.0.4. This is due to the plugin not properly validating a user's capabilities prior to updating their profile in the el_update_profile() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change their capabilities to those of an administrator.	8.8	More Details
CVE-2025-55454	An authenticated arbitrary file upload vulnerability in the component /msg/sendfiles of DooTask v1.0.51 allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2025-55370	Incorrect access control in the component \controller\ResourceController.java of jshERP v3.5 allows unauthorized attackers to obtain all the corresponding ID data by modifying the ID value.	8.8	More Details
CVE-2025-57731	In JetBrains YouTrack before 2025.2.92387 stored XSS was possible via Mermaid diagram content	8.7	More Details
CVE-2025-28041	Incorrect access control in the doFilter function of itranswarp up to 2.19 allows attackers to access sensitive components without authentication.	8.6	More Details
CVE-2025-30256	A denial of service vulnerability exists in the HTTP Header Parsing functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted series of HTTP requests can lead to a reboot. An attacker can send multiple network packets to trigger this vulnerability.	8.6	More Details
CVE-2025-43960	Adminer 4.8.1, when using Monolog for logging, allows a Denial of Service (memory consumption) via a crafted serialized payload (e.g., using s:1000000000), leading to a PHP Object Injection issue. Remote, unauthenticated attackers can trigger this by sending a malicious serialized object, which forces excessive memory usage, rendering Adminer’s interface unresponsive and causing a server-level DoS. While the server may recover after several minutes, multiple simultaneous requests can cause a complete crash requiring manual intervention.	8.6	More Details

CVE-2025-5260	Server-Side Request Forgery (SSRF) vulnerability in Pik Online Yazılım Çözümleri A.Ş. Pik Online allows Server Side Request Forgery.This issue affects Pik Online: before 3.1.5.	8.6	More Details
CVE-2025-48158	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Alex Githatu BuddyPress XProfile Custom Image Field allows Path Traversal. This issue affects BuddyPress XProfile Custom Image Field: from n/a through 3.0.1.	8.6	More Details
CVE-2025-53418	Delta Electronics COMMGR has Stack-based Buffer Overflow vulnerability.	8.6	More Details
CVE-2025-55383	Moss before v0.15 has a file upload vulnerability. The "upload" function configuration allows attackers to upload files of any extension to any location on the target server.	8.6	More Details
CVE-2025-52451	Improper Input Validation vulnerability in Salesforce Tableau Server on Windows, Linux (tabdoc api - create-data-source-from-file-upload modules) allows Absolute Path Traversal.This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	8.5	More Details
CVE-2025-53194	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Crocoblock JetEngine allows Code Injection. This issue affects JetEngine: from n/a through 3.7.0.	8.5	More Details
CVE-2025-56216	phpgurukul Hospital Management System 4.0 is vulnerable to SQL Injection in about-us.php via the pagetitle parameter.	8.5	More Details
CVE-2025-7051	On N-central, it is possible for any authenticated user to read, write and modify syslog configuration across customers on an N-central server. This vulnerability is present in all deployments of N-central prior to 2025.2.	8.3	More Details
CVE-2025-52461	An out-of-bounds read vulnerability exists in the Nex parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted .nex file can lead to an information leak. An attacker can provide a malicious file to trigger this vulnerability.	8.2	More Details
CVE-2025-54031	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Schiocco Support Board allows PHP Local File Inclusion. This issue affects Support Board: from n/a through 3.8.0.	8.1	More Details
CVE-2025-51605	An issue was discovered in Shopizer 3.2.7. The server's CORS implementation reflects the client-supplied Origin header verbatim into Access-Control-Allow-Origin without any whitelist validation, while also enabling Access-Control-Allow-Credentials: true. This allows any malicious origin to make authenticated cross-origin requests and read sensitive responses.	8.1	More Details
CVE-2025-9048	The Wptobe-memberships plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the del_img_ajax_call() function in all versions up to, and including, 3.4.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.1	More Details
CVE-2025-5060	The Bravis User plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.0. This is due to the plugin not properly logging a user in with the data that was previously verified through the facebook_ajax_login_callback(). This makes it possible for unauthenticated attackers to log in as administrative users, as long as they have an existing account on the site, and access to the administrative user's email.	8.1	More Details
CVE-2025-48149	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in dedalx Cook&Meal allows PHP Local File Inclusion. This issue affects Cook&Meal: from n/a through 1.2.3.	8.1	More Details
CVE-2025-48157	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Michele Giorgi Formality allows PHP Local File Inclusion. This issue affects Formality: from n/a through 1.5.9.	8.1	More Details
CVE-2025-48160	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CocoBasic Caliris allows PHP Local File Inclusion. This issue affects Caliris: from n/a through 1.5.	8.1	More Details
CVE-2025-8592	The Inspiro theme for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.2. This is due to missing or incorrect nonce validation on the inspiro_install_plugin() function. This makes it possible for unauthenticated attackers to install plugins from the repository via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.1	More Details
CVE-2025-57771	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. In versions prior to 3.25.5, Roo-Code fails to properly handle process substitution and single ampersand characters in the command parsing logic for auto-execute commands. If a user has enabled auto-approved execution for a command such as ls, an attacker who can submit crafted prompts to the agent may inject arbitrary commands to be executed alongside the intended command. Exploitation requires attacker access to submit prompts and for the user to have enabled auto-approved command execution, which is disabled by default. This vulnerability could allow an attacker to execute arbitrary code. The issue is fixed in version 3.25.5.	8.1	More Details
CVE-2025-55741	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. In versions 0.3.0 and earlier, users without the Delete privilege for products are unable to delete individual products via the standard endpoint, as expected. However, these users can bypass intended access controls by issuing requests to the mass-delete endpoint, allowing them to delete products without proper authorization. This vulnerability allows unauthorized product deletion, leading to potential data loss and business disruption. The issue is fixed in version 0.3.1. No known workarounds exist.	8.1	More Details
CVE-2025-46411	A stack-based buffer overflow vulnerability exists in the MFER parsing functionality of The Biosig Project libbiosig 3.9.0 and Master Branch (35a819fa). A specially crafted MFER file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details

CVE-2025-48171	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in thembay Cena Store allows PHP Local File Inclusion. This issue affects Cena Store: from n/a through 2.11.26.	8.1	More Details
CVE-2024-50641	An authentication bypass vulnerability in PandoraNext-TokensTool v0.6.8 and before. An attacker can exploit this vulnerability to access API without any token.	8.1	More Details
CVE-2025-32010	A stack-based buffer overflow vulnerability exists in the Cloud API functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted HTTP response can lead to arbitrary code execution. An attacker can send an HTTP response to trigger this vulnerability.	8.1	More Details
CVE-2025-8309	There is an improper privilege management vulnerability identified in ManageEngine's Asset Explorer, ServiceDesk Plus, ServiceDesk Plus MSP, and SupportCenter Plus products by Zohocorp. This vulnerability impacts Asset Explorer versions before 7710, ServiceDesk Plus versions before 15110, ServiceDesk Plus MSP versions before 14940, and SupportCenter Plus versions before 14940.	8.1	More Details
CVE-2025-24322	An unsafe default authentication vulnerability exists in the Initial Setup Authentication functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted network request can lead to arbitrary code execution. An attacker can browse to the device to trigger this vulnerability.	8.1	More Details
CVE-2025-53207	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WP Travel WP Travel Gutenberg Blocks allows PHP Local File Inclusion. This issue affects WP Travel Gutenberg Blocks: from n/a through 3.9.0.	8.1	More Details
CVE-2025-35115	Agiloft Release 28 downloads critical system packages over an insecure HTTP connection. An attacker in a Man-In-the-Middle position could replace or modify the contents of the download URL. Users should upgrade to Agiloft Release 30.	8.1	More Details
CVE-2025-27215	An Improper Access Control could allow a malicious actor authenticated in the API of certain UniFi Connect Display Cast devices to make unsupported changes to the system. Affected Products: UniFi Connect Display Cast (Version 1.10.3 and earlier) UniFi Connect Display Cast Pro (Version 1.0.89 and earlier) UniFi Connect Display Cast Lite (Version 1.0.3 and earlier) Mitigation: Update UniFi Connect Display Cast to Version 1.10.7 or later Update UniFi Connect Display Cast Pro to Version 1.0.94 or later Update UniFi Connect Display Cast Lite to Version 1.1.8 or later	8.1	More Details
CVE-2025-53198	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in favethemes Houzez allows PHP Local File Inclusion. This issue affects Houzez: from n/a through 4.0.4.	8.1	More Details
CVE-2025-53567	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in nK Ghost Kit allows PHP Local File Inclusion. This issue affects Ghost Kit: from n/a through 3.4.1.	8.1	More Details
CVE-2025-53565	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RadiusTheme Widget for Google Reviews allows PHP Local File Inclusion. This issue affects Widget for Google Reviews: from n/a through 1.0.15.	8.1	More Details
CVE-2025-53204	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ovatheme eventlist allows PHP Local File Inclusion. This issue affects eventlist: from n/a through 1.9.2.	8.1	More Details
CVE-2025-55742	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. Before 0.2.1, UnoPim contains a stored cross-site scripting vulnerability via SVG MIME/sanitizer bypass in the /admin/settings/users/create endpoint. This vulnerability is fixed in 0.2.1.	8.0	More Details
CVE-2025-36174	IBM Integrated Analytics System 1.0.0.0 through 1.0.30.0 could allow an authenticated user to upload a file with dangerous types that could be executed by another user if opened.	8.0	More Details
CVE-2025-23313	NVIDIA NeMo Framework for all platforms contains a vulnerability in the NLP component, where malicious data created by 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-2024-56179	In MindManager Windows versions prior to 24.1.150, attackers could potentially write to unexpected directories in victims' machines via directory traversal if victims opened file attachments located in malicious mmap files.	7.8	More Details
CVE-2025-9380	A vulnerability was identified in FNKvision Y215 CCTV Camera 10.194.120.40. Affected by this issue is some unknown functionality of the file /etc/passwd of the component Firmware. Such manipulation leads to hard-coded credentials. Local access is required to approach this attack. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2025-23315	NVIDIA NeMo Framework for all platforms contains a vulnerability in the export and deploy component, where malicious data created by 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-2025-33120	IBM QRadar SIEM 7.5 through 7.5.0 UP13 could allow an authenticated user to escalate their privileges via a misconfigured cronjob due to execution with unnecessary privileges.	7.8	More Details
CVE-2025-38743	Dell iDRAC Service Module (iSM), versions prior to 6.0.3.0, contains a Buffer Access with Incorrect Length Value vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Elevation of privileges.	7.8	More Details
CVE-2025-23314	NVIDIA NeMo Framework for all platforms contains a vulnerability in the NLP component, where malicious data created by 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-			

2025-50674	An issue was discovered in the changePassword method in file /usr/share/php/openmediavault/system/user.inc in OpenMediaVault 7.4.17 allowing local authenticated attackers to escalate privileges to root.	7.8	More Details
CVE-2025-23312	NVIDIA NeMo Framework for all platforms contains a vulnerability in the retrieval services component, where malicious data created by an attacker could cause a code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-52094	Insecure Permissions vulnerability in PDQ Smart Deploy V.3.0.2040 allows a local attacker to execute arbtirary code via the \HKLM\SYSTEM\Setup\SmartDeploy component	7.8	More Details
CVE-2025-1994	IBM Cognos Command Center 10.2.4.1 and 10.2.5 could allow a local user to execute arbitrary code on the system due to the use of unsafe use of the BinaryFormatter function.	7.8	More Details
CVE-2025-55230	Untrusted pointer dereference in Windows MBT Transport driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-53419	Delta Electronics COMMGR has Code Injection vulnerability.	7.8	More Details
CVE-2025-23307	NVIDIA NeMo Curator for all platforms contains a vulnerability where a malicious file created by an attacker could allow code injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-48988	SQL Injection vulnerability in Apache StreamPark. This issue affects Apache StreamPark: from 2.1.4 before 2.1.6. Users are recommended to upgrade to version 2.1.6, which fixes the issue. This vulnerability is present only in the distribution package (SpringBoot platform) and does not involve Maven artifacts. It can only be exploited after a user has successfully logged into the platform (implying that the attacker would first need to compromise the login authentication). As a result, the associated risk is considered relatively low.	7.6	More Details
CVE-2025-48298	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Benjamin Denis SEOPress for MainWP allows PHP Local File Inclusion. This issue affects SEOPress for MainWP: from n/a through 1.4.	7.5	More Details
CVE-2025-55498	Tenda AC6 V15.03.06.23_multi was discovered to contain a buffer overflow via the time parameter in the fromSetSysTime function.	7.5	More Details
CVE-2025-24496	An information disclosure vulnerability exists in the /goform/getproductInfo functionality of Tenda AC6 V5.0 V02.03.01.110. Specially crafted network packets can lead to a disclosure of sensitive information. An attacker can send packets to trigger this vulnerability.	7.5	More Details
CVE-2025-55482	Tenda AC6 V15.03.06.23_multi is vulnerable to Buffer Overflow in the formSetCfm function.	7.5	More Details
CVE-2025-9255	WebITR developed by Uniong has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2025-35114	Agiloft Release 28 contains several accounts with default credentials that could allow local privilege escalation. The password hash is known for at least one of the accounts and the credentials could be cracked offline. Users should upgrade to Agiloft Release 30.	7.5	More Details
CVE-2025-48302	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Roxnor FundEngine allows PHP Local File Inclusion. This issue affects FundEngine: from n/a through 1.7.4.	7.5	More Details
CVE-2025-54925	CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists that could cause unauthorized access to sensitive data when an attacker configures the application to access a malicious url.	7.5	More Details
CVE-2025-55483	Tenda AC6 V15.03.06.23_multi is vulnerable to Buffer Overflow in the function formSetMacFilterCfg via the parameters macFilterType and deviceList.	7.5	More Details
CVE-2025-54924	CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists that could cause unauthorized access to sensitive data when an attacker sends a specially crafted document to a vulnerable endpoint.	7.5	More Details
CVE-2025-57803	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-28 and 7.1.2-2 for ImageMagick's 32-bit build, a 32-bit integer overflow in the BMP encoder’s scanline-stride computation collapses bytes_per_line (stride) to a tiny value while the per-row writer still emits 3 × width bytes for 24-bpp images. The row base pointer advances using the (overflowed) stride, so the first row immediately writes past its slot and into adjacent heap memory with attacker-controlled bytes. This is a classic, powerful primitive for heap corruption in common auto-convert pipelines. This issue has been patched in versions 6.9.13-28 and 7.1.2-2.	7.5	More Details
CVE-2025-55603	Tenda AX3 V16.03.12.10_CN is vulnerable to Buffer Overflow in the fromSetSysTime function via the ntpServer parameter.	7.5	More Details
CVE-2024-53494	Incorrect access control in the preHandle function of SpringBootBlog v1.0.0 allows attackers to access sensitive components without authentication.	7.5	More Details
CVE-			

2025-55602	D-Link DIR-619L 2.06B01 is vulnerable to Buffer Overflow in the formSysCmd function via the submit-url parameter.	7.5	More Details
CVE-2025-55631	Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 was discovered to manage users' sessions system wide instead of an account-by-account basis, potentially leading to a Denial of Service (DoS) via resource exhaustion.	7.5	More Details
CVE-2025-55634	Incorrect access control in the RTMP server settings of Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 allows unauthorized attackers to cause a Denial of Service (DoS) via initiating a large number of simultaneous ffmpeg-based stream pushes.	7.5	More Details
CVE-2025-55599	D-Link DIR-619L 2.06B01 is vulnerable to Buffer Overflow in the formWlanSetup function via the parameter f_wds_wepKey.	7.5	More Details
CVE-2024-57152	Incorrect access control in the preHandle function of my-site v1.0.2 allows attackers to access sensitive components without authentication via the cn.luischen.interceptor.BaseInterceptor class	7.5	More Details
CVE-2024-53495	Incorrect access control in the preHandle function of my-site v1.0.2.RELEASE allows attackers to access sensitive components without authentication.	7.5	More Details
CVE-2025-54813	Improper Output Neutralization for Logs vulnerability in Apache Log4cxx. When using JSONLayout, not all payload bytes are properly escaped. If an attacker-supplied message contains certain non-printable characters, these will be passed along in the message and written out as part of the JSON message. This may prevent applications that consume these logs from correctly interpreting the information within them. This issue affects Apache Log4cxx: before 1.5.0. Users are recommended to upgrade to version 1.5.0, which fixes the issue.	7.5	More Details
CVE-2025-30975	Improper Control of Generation of Code ('Code Injection') vulnerability in SaifuMak Add Custom Codes allows Code Injection. This issue affects Add Custom Codes: from n/a through 4.80.	7.5	More Details
CVE-2023-47799	Mahara before 22.10.4 and 23.x before 23.04.4 allows information disclosure if the experimental HTML bulk export is used via the administration interface or via the CLI, and the resulting export files are given to the account holders. They may contain images of other account holders because the cache is not cleared after the files of one account are exported.	7.5	More Details
CVE-2025-8289	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.2.4 via deserialization of untrusted input in the delete_associated_files function. This makes it possible for unauthenticated attackers to inject a PHP Object. This vulnerability may be exploited by unauthenticated attackers when a form is present on the site with a file upload action, and doesn't affect sites with PHP version > 8. This vulnerability also requires the 'Redirection For Contact Form 7 Extension - Create Post' extension to be installed and activated in order to be exploited. 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. We confirmed there is a usable gadget in Contact Form 7 plugin that makes arbitrary file deletion possible when installed with this plugin. Given Contact Form 7 is a requirement of this plugin, it is likely that any site with this plugin and the 'Redirection For Contact Form 7 Extension - Create Post' extension enabled is vulnerable to arbitrary file deletion.	7.5	More Details
CVE-2025-55298	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to ImageMagick versions 6.9.13-28 and 7.1.2-2, a format string bug vulnerability exists in InterpretImageFilename function where user input is directly passed to FormatLocaleString without proper sanitization. An attacker can overwrite arbitrary memory regions, enabling a wide range of attacks from heap overflow to remote code execution. This issue has been patched in versions 6.9.13-28 and 7.1.2-2.	7.5	More Details
CVE-2025-55732	Frappe is a full-stack web application framework. Prior to 15.74.2 and 14.96.15, an attacker could implement SQL injection through specially crafted requests, allowing malicious people to access sensitive information. This vulnerability is a bypass of the official patch released for CVE-2025-52895. This vulnerability is fixed in 15.74.2 and 14.96.15.	7.5	More Details
CVE-2025-55605	Tenda AX3 V16.03.12.10_CN is vulnerable to Buffer Overflow in the saveParentControlInfo function via the deviceName parameter.	7.5	More Details
CVE-2025-55606	Tenda AX3 V16.03.12.10_CN is vulnerable to Buffer Overflow in the fromAdvSetMacMtuWan function via the serverName parameter.	7.5	More Details
CVE-2025-55611	D-Link DIR-619L 2.06B01 is vulnerable to Buffer Overflow in the formLanguageChange function via the nextPage parameter.	7.5	More Details
CVE-2025-9172	The Vibes plugin for WordPress is vulnerable to time-based SQL Injection via the ‘resource’ parameter in all versions up to, and including, 2.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2025-48978	An Improper Input Validation in EdgeMAX EdgeSwitch (Version 1.11.0 and earlier) could allow a Command Injection by a malicious actor with access to EdgeSwitch adjacent network. Affected Products: EdgeMAX EdgeSwitch (Version 1.11.0 and earlier) Mitigation: Update the EdgeMAX EdgeSwitch to Version 1.11.1 or later.	7.5	More Details
CVE-2025-54028	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Saleswonder Team Tobias CF7 WOW Styler allows PHP Local File Inclusion. This issue affects CF7 WOW Styler: from n/a through 1.7.2.	7.5	More Details
CVE-2025-6188	On affected platforms running Arista EOS, maliciously formed UDP packets with source port 3503 may be accepted by EOS. UDP Port 3503 is associated with LspPing Echo Reply. This can result in unexpected behaviors, especially for UDP based services that do not perform some form of authentication.	7.5	More Details

CVE-2025-55564	Tenda AC15 v15.03.05.19_multi_TD01 has a stack overflow via the list parameter in the fromSetIpMacBind function.	7.5	More Details
CVE-2025-5261	Authorization Bypass Through User-Controlled Key vulnerability in Pik Online Yazılım Çözümleri A.Ş. Pik Online allows Exploitation of Trusted Identifiers.This issue affects Pik Online: before 3.1.5.	7.5	More Details
CVE-2025-55715	Insertion of Sensitive Information Into Sent Data vulnerability in Themeisle Otter - Gutenberg Block allows Retrieve Embedded Sensitive Data. This issue affects Otter - Gutenberg Block: from n/a through 3.1.0.	7.5	More Details
CVE-2025-52194	A buffer overflow vulnerability exists in libsndfile version 1.2.2 and potentially earlier versions when processing malformed IRCAM audio files. The vulnerability occurs in the ircam_read_header function at src/ircam.c:164 during sample rate processing, leading to memory corruption and potential code execution.	7.5	More Details
CVE-2025-53208	Authorization Bypass Through User-Controlled Key vulnerability in paymayapg Maya Business allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Maya Business: from n/a through 1.2.0.	7.5	More Details
CVE-2025-48956	vLLM is an inference and serving engine for large language models (LLMs). From 0.1.0 to before 0.10.1.1, a Denial of Service (DoS) vulnerability can be triggered by sending a single HTTP GET request with an extremely large header to an HTTP endpoint. This results in server memory exhaustion, potentially leading to a crash or unresponsiveness. The attack does not require authentication, making it exploitable by any remote user. This vulnerability is fixed in 0.10.1.1.	7.5	More Details
CVE-2025-57732	In JetBrains TeamCity before 2025.07.1 privilege escalation was possible due to incorrect directory ownership	7.5	More Details
CVE-2025-54750	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in FunnelKit Funnel Builder by FunnelKit allows PHP Local File Inclusion. This issue affects Funnel Builder by FunnelKit: from n/a through 3.11.1.	7.5	More Details
CVE-2025-54017	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Cozmoslabs Paid Member Subscriptions allows PHP Local File Inclusion. This issue affects Paid Member Subscriptions: from n/a through 2.15.4.	7.5	More Details
CVE-2025-53210	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in bdthemes ZoloBlocks allows PHP Local File Inclusion. This issue affects ZoloBlocks: from n/a through 2.3.2.	7.5	More Details
CVE-2025-27721	Unauthorized users can access INFINITT PACS System Manager without proper authorization, which could lead to unauthorized access to system resources.	7.5	More Details
CVE-2025-54021	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mitchell Bennis Simple File List allows Path Traversal. This issue affects Simple File List: from n/a through 6.1.14.	7.5	More Details
CVE-2025-54052	Cross-Site Request Forgery (CSRF) vulnerability in Realtyna Realtyna Organic IDX plugin allows PHP Local File Inclusion. This issue affects Realtyna Organic IDX plugin: from n/a through 5.0.0.	7.5	More Details
CVE-2025-29421	PerfreeBlog v4.0.11 has an arbitrary file read vulnerability in the getThemeFileContent function.	7.5	More Details
CVE-2025-53119	An unauthenticated unrestricted file upload vulnerability allows an attacker to upload malicious binaries and scripts to the server.	7.5	More Details
CVE-2025-29420	PerfreeBlog v4.0.11 has a directory traversal vulnerability in the getThemeFilesByName function.	7.5	More Details
CVE-2025-54034	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Tribulant Software Newsletters allows PHP Local File Inclusion. This issue affects Newsletters: from n/a through 4.10.	7.5	More Details
CVE-2025-55231	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Storage allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2025-2697	IBM Cognos Command Center 10.2.4.1 and 10.2.5 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	7.4	More Details
CVE-2025-9471	A vulnerability has been found in itsourcecode Apartment Management System 1.0. This vulnerability affects unknown code of the file /maintenance/add_maintenance_cost.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-55581	D-Link DCS-825L firmware version 1.08.01 and possibly prior versions contain an insecure implementation in the mydlink-watch-dog.sh script. The script monitors and respawns the `dcp` and `signalc` binaries without validating their integrity, origin, or permissions. An attacker with filesystem access (e.g., via UART or firmware modification) may replace these binaries to achieve persistent arbitrary code execution with root privileges. The issue stems from improper handling of executable trust and absence of integrity checks in the watchdog logic.	7.3	More Details

CVE-2025-9238	A vulnerability was determined in Swatadru Exam-Seating-Arrangement up to 97335ccebf95468d92525f4255a2241d2b0b002f. Affected is an unknown function of the file /student.php of the component Student Login. Executing manipulation of the argument email can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-9307	A flaw has been found in PHPGurukul Online Course Registration 3.1. This affects an unknown function of the file /admin/session.php. This manipulation of the argument sesssion causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-26497	Unrestricted Upload of File with Dangerous Type vulnerability in Salesforce Tableau Server on Windows, Linux (Flow Editor modules) allows Absolute Path Traversal.This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	7.3	More Details
CVE-2025-26498	Unrestricted Upload of File with Dangerous Type vulnerability in Salesforce Tableau Server on Windows, Linux (establish-connection-no-undo modules) allows Absolute Path Traversal.This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	7.3	More Details
CVE-2025-9472	A vulnerability was found in itsourcecode Apartment Management System 1.0. This issue affects some unknown processing of the file /owner_utility/add_owner_utility.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-9426	A weakness has been identified in itsourcecode Online Tour and Travel Management System 1.0. This affects an unknown part of the file /package.php. Executing manipulation of the argument subcatid can lead to sql injection. The attack may be performed from a remote location. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-9423	A vulnerability was determined in Campcodes Online Water Billing System 1.0. Affected is an unknown function of the file /editecex.php. This manipulation of the argument ID 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-2025-9311	A vulnerability was identified in itsourcecode Apartment Management System 1.0. Affected by this issue is some unknown functionality of the file /fair/addfair.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-9425	A security flaw has been discovered in itsourcecode Online Tour and Travel Management System 1.0. Affected by this issue is some unknown functionality of the file /enquiry.php. Performing manipulation of the argument pid 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.	7.3	More Details
CVE-2025-9470	A flaw has been found in itsourcecode Apartment Management System 1.0. This affects an unknown part of the file /management/add_m_committee.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-55503	Tenda AC6 V15.03.06.23_multi has a stack overflow vulnerability via the deviceName parameter in the saveParentControlInfo function.	7.3	More Details
CVE-2025-9421	A vulnerability has been found in itsourcecode Apartment Management System 1.0. This affects an unknown function of the file /complain/addcomplain.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-55630	A discrepancy in the error message returned by the login function of Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 when entering the wrong username and password allows attackers to enumerate existing accounts.	7.3	More Details
CVE-2025-9444	A vulnerability has been found in 1000projects Online Project Report Submission and Evaluation System 1.0. This issue affects some unknown processing of the file /admin/controller/delete_group_student.php. The manipulation of the argument batch_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-55524	Insecure permissions in Agent-Zero v0.8.* allow attackers to arbitrarily reset the system via unspecified vectors.	7.3	More Details
CVE-2025-9418	A security vulnerability has been detected in itsourcecode Apartment Management System 1.0. Impacted is an unknown function of the file /owner/addowner.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9492	A vulnerability was determined in Campcodes Online Water Billing System 1.0. This affects an unknown function of the file /addclient1.php. Executing manipulation of the argument lname can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. Other parameters might be affected as well.	7.3	More Details
CVE-2025-9476	A vulnerability has been found in SourceCodester Human Resource Information System 1.0. Affected by this issue is some unknown functionality of the file /Superadmin_Dashboard/process/editemployee_process.php. Such manipulation of the argument employee_file201 leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-9419	A vulnerability was detected in itsourcecode Apartment Management System 1.0. The affected element is an unknown function of the file /unit/addunit.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-9305	A security vulnerability has been detected in SourceCodester Online Bank Management System 1.0. The affected element is an unknown function of the file /bank/mnotice.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9302	A vulnerability was identified in PHPGurukul User Management System 1.0. This vulnerability affects unknown code of the file /signup.php. Such manipulation of the argument emailid 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-	A flaw has been found in SourceCodester Human Resource Information System 1.0. Affected by this vulnerability is an unknown functionality of the file /Admin_Dashboard/process/editemployee_process.php. This manipulation of the argument employee_file201	7.3	More

9475	causes unrestricted upload. The attack may be initiated remotely. The exploit has been published and may be used.		Details
CVE-2025-9420	A flaw has been found in itsourcecode Apartment Management System 1.0. The impacted element is an unknown function of the file /floor/addfloor.php. Executing manipulation of the argument hdnid can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-9304	A weakness has been identified in SourceCodester Online Bank Management System 1.0. Impacted is an unknown function of the file /bank/show.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from a remote location. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-9473	A security vulnerability has been detected in SourceCodester Online Bank Management System 1.0. This impacts an unknown function of the file /feedback.php. The manipulation of the argument msg 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-2025-9468	A security vulnerability has been detected in itsourcecode Apartment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /bill/add_bill.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-9469	A vulnerability was detected in itsourcecode Apartment Management System 1.0. Affected by this issue is some unknown functionality of the file /fund/add_fund.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-36729	A non-primary administrator user with admin rights to the web interface but without shell access permissions can display configuration of the device including the master admin password. This vulnerability also allows the user to give themselves shell access with the root gid.	7.2	More Details
CVE-2025-7813	The Events Calendar, Event Booking, Registrations and Event Tickets – Eventin plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.0.37 via the proxy_image function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.2	More Details
CVE-2025-54926	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause remote code execution when an authenticated attacker with admin privileges uploads a malicious file over HTTP which then gets executed.	7.2	More Details
CVE-2025-49438	Deserialization of Untrusted Data vulnerability in Max Chirkov Simple Login Log allows Object Injection. This issue affects Simple Login Log: from n/a through 1.1.3.	7.2	More Details
CVE-2025-6737	Securden’s Unified PAM Remote Vendor Gateway access portal shares infrastructure and access tokens across multiple tenants. A malicious actor can obtain authentication material and access the gateway server with low-privilege permissions.	7.2	More Details
CVE-2025-54012	Deserialization of Untrusted Data vulnerability in nanbu Welcart e-Commerce allows Object Injection. This issue affects Welcart e-Commerce: from n/a through 2.11.16.	7.2	More Details
CVE-2025-29523	D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the ping6 function.	7.2	More Details
CVE-2025-29516	D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the backup function.	7.2	More Details
CVE-2025-9379	A vulnerability was determined in Belkin AX1800 1.1.00.016. Affected by this vulnerability is an unknown functionality of the component Firmware Update Handler. This manipulation causes insufficient verification of data authenticity. The attack can be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2025-4650	User with high privileges is able to introduce a SQLi using the Meta Service indicator page. Caused by an Improper Neutralization of Special Elements used in an SQL Command.This issue affects web: from 24.10.0 before 24.10.9, from 24.04.0 before 24.04.16, from 23.10.0 before 23.10.26.	7.2	More Details
CVE-2025-31355	A firmware update vulnerability exists in the Firmware Signature Validation functionality of Tenda AC6 V5.0 V02.03.01.110. A specially crafted malicious file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.2	More Details
CVE-2025-53562	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player - Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Universal Video Player - Addon for WPBakery Page Builder: from n/a through 3.2.1.	7.1	More Details
CVE-2025-54027	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Schiocco Support Board allows Reflected XSS. This issue affects Support Board: from n/a through 3.8.0.	7.1	More Details
CVE-2025-53563	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Youtube Vimeo Video Player and Slider allows Reflected XSS. This issue affects Youtube Vimeo Video Player and Slider: from n/a through 3.8.	7.1	More Details
CVE-2025-53564	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup HTML5 Radio Player - WPBakery Page Builder Addon allows Reflected XSS. This issue affects HTML5 Radio Player - WPBakery Page Builder Addon: from n/a through 2.5.	7.1	More Details
CVE-2025-53226	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in digitalzoomstudio Comments Capcha Box allows Reflected XSS. This issue affects Comments Capcha Box: from n/a through 1.1.	7.1	More Details
CVE-			

2025-53212	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Revolution Video Player With Bottom Playlist allows Reflected XSS. This issue affects Revolution Video Player With Bottom Playlist: from n/a through 2.9.2.	7.1	More Details
CVE-2025-54460	The vulnerability, if exploited, could allow an authenticated miscreant (with privileges to create or access publication targets of type Text File or HDFS) to upload and persist files that could potentially be executed.	7.1	More Details
CVE-2025-48159	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Youtube Vimeo Video Player and Slider WP Plugin allows Reflected XSS. This issue affects Youtube Vimeo Video Player and Slider WP Plugin: from n/a through 3.8.	7.1	More Details
CVE-2025-28977	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress WP Pipes allows Reflected XSS. This issue affects WP Pipes: from n/a through 1.4.3.	7.1	More Details
CVE-2025-48162	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in quantumcloud Simple Business Directory Pro allows Reflected XSS. This issue affects Simple Business Directory Pro: from n/a through 15.5.1.	7.1	More Details
CVE-2025-8281	The WP Talroo WordPress plugin through 2.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin and unauthenticated users.	7.1	More Details
CVE-2025-48297	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in quantumcloud Simple Link Directory allows Reflected XSS. This issue affects Simple Link Directory: from n/a through n/a.	7.1	More Details
CVE-2025-48296	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup UpStore allows Reflected XSS. This issue affects UpStore: from n/a through 1.7.0.	7.1	More Details
CVE-2025-48170	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player - Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Universal Video Player - Addon for WPBakery Page Builder: from n/a through 3.2.1.	7.1	More Details
CVE-2025-53201	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster allows Reflected XSS. This issue affects Jobmonster: from n/a through 4.7.8.	7.1	More Details
CVE-2025-53205	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Radio Player Shoutcast & Icecast allows Reflected XSS. This issue affects Radio Player Shoutcast & Icecast: from n/a through 4.4.7.	7.1	More Details
CVE-2025-54032	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace Real Estate Manager Pro allows Reflected XSS. This issue affects Real Estate Manager Pro: from n/a through 12.7.3.	7.1	More Details
CVE-2025-48163	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup SHOUT - HTML5 Radio Player With Ads - ShoutCast and IceCast Support allows Reflected XSS. This issue affects SHOUT - HTML5 Radio Player With Ads - ShoutCast and IceCast Support: from n/a through 3.5.4.	7.1	More Details
CVE-2025-48168	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Apollo - Sticky Full Width HTML5 Audio Player allows Reflected XSS. This issue affects Apollo - Sticky Full Width HTML5 Audio Player: from n/a through 3.4.	7.1	More Details
CVE-2025-53319	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Raptive Raptive Ads allows Reflected XSS. This issue affects Raptive Ads: from n/a through 3.8.0.	7.1	More Details
CVE-2025-48154	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Multimedia Playlist Slider Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Multimedia Playlist Slider Addon for WPBakery Page Builder: from n/a through 2.1.	7.1	More Details
CVE-2025-54044	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in _CreativeMedia_ Elite Video Player allows Reflected XSS. This issue affects Elite Video Player: from n/a through 10.0.5.	7.1	More Details
CVE-2025-48151	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Map Locations allows Reflected XSS. This issue affects CM Map Locations: from n/a through 2.1.6.	7.1	More Details
CVE-2025-48152	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dimafreund Rentsyst allows Reflected XSS. This issue affects Rentsyst: from n/a through 2.0.100.	7.1	More Details
CVE-2025-54670	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bobbingwide oik allows Reflected XSS. This issue affects oik: from n/a through 4.15.2.	7.1	More Details
CVE-2025-53559	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player - Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Universal Video Player - Addon for WPBakery Page Builder: from n/a through 3.2.1.	7.1	More Details
CVE-2025-54055	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Druco allows Reflected XSS. This issue affects Druco: from n/a through 1.5.2.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Responsive HTML5		

2025-54056	Audio Player PRO With Playlist allows Reflected XSS. This issue affects Responsive HTML5 Audio Player PRO With Playlist: from n/a through 3.5.8.	7.1	More Details
CVE-2025-51989	HTML injection vulnerability in the registration interface in Evolution Consulting Kft. HRmaster module v235 allows an attacker to inject HTML tags into the "keresztnév" (firstname) field, which will be sent out in an email resulting in possible Phishing scenarios against any, previously not registered, email address.	7.0	More Details
CVE-2025-51281	D-Link DI-8100 16.07.26A1 is vulnerable to Buffer Overflow via the en`, `val and id parameters in the qj_asp function. This vulnerability allows authenticated attackers to cause a Denial of Service (DoS) by sending crafted GET requests with overly long values for these parameters.	7.0	More Details
CVE-2025-36530	Mattermost versions 10.9.x <= 10.9.1, 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17 fail to properly validate file paths during plugin import operations which allows restricted admin users to install unauthorized custom plugins via path traversal in the import functionality, bypassing plugin signature enforcement and marketplace restrictions.	6.8	More Details
CVE-2025-49222	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.9.x <= 10.9.2, 10.10.x <= 10.10.0 fail to validate upload types in remote cluster upload sessions which allows a system admin to upload non-attachment file types via shared channels that could potentially be placed in arbitrary filesystem directories.	6.8	More Details
CVE-2025-8023	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.9.x <= 10.9.2 fails to sanitize path traversal sequences in template file destination paths, which allows a system admin to perform path traversal attacks via malicious path components, potentially enabling malicious file placement outside intended directories.	6.8	More Details
CVE-2025-29517	D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the traceroute6 function.	6.8	More Details
CVE-2025-55301	The Scratch Channel is a news website. In version 1, it is possible to go to application in devtools and click local storage to edit the account's username locally. This issue has been patched in version 1.1.	6.7	More Details
CVE-2025-8453	CWE-269: Improper Privilege Management vulnerability exists that could cause privilege escalation and arbitrary code execution when a privileged engineer user with console access modifies a configuration file used by a root-level daemon to execute custom scripts.	6.7	More Details
CVE-2025-54053	Deserialization of Untrusted Data vulnerability in Adrian Tobey Groundhogg allows Object Injection. This issue affects Groundhogg: from n/a through 4.2.2.	6.6	More Details
CVE-2025-50860	SQL Injection in the listdomains function in Easy Hosting Control Panel (EHCP) 20.04.1.b allows authenticated attackers to access or manipulate database contents via the arananalan POST parameter.	6.5	More Details
CVE-2025-41415	The vulnerability, if exploited, could allow an authenticated miscreant (with privileges to access publication targets) to retrieve sensitive information that could then be used to gain additional access to downstream resources.	6.5	More Details
CVE-2025-55521	An issue in the component /settings/localisation of Akaunting v3.1.18 allows authenticated attackers to cause a Denial of Service (DoS) via a crafted POST request.	6.5	More Details
CVE-2025-57764	WeGIA is a Web manager for charitable institutions. Prior to 3.4.7, a Reflected Cross-Site Scripting (XSS) vulnerability was identified in the cargos.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the msg_e parameter. This vulnerability is fixed in 3.4.7.	6.5	More Details
CVE-2025-57765	WeGIA is a Web manager for charitable institutions. Prior to 3.4.7, a Reflected Cross-Site Scripting (XSS) vulnerability was identified in the pre_cadastro_adotante.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the msg_e parameter. This vulnerability is fixed in 3.4.7.	6.5	More Details
CVE-2025-51825	JeecgBoot versions from 3.4.3 up to 3.8.0 were found to contain a SQL injection vulnerability in the /jeecg-boot/online/cgreport/head/parseSql endpoint, which allows bypassing SQL blacklist restrictions.	6.5	More Details
CVE-2025-9259	WebITR developed by Uniong has an Arbitrary File Reading vulnerability, allowing remote attackers with regular privileges to exploit Absolute Path Traversal to download arbitrary system files.	6.5	More Details
CVE-2025-9258	WebITR developed by Uniong has an Arbitrary File Reading vulnerability, allowing remote attackers with regular privileges to exploit Absolute Path Traversal to download arbitrary system files.	6.5	More Details
CVE-2025-9256	WebITR developed by Uniong has an Arbitrary File Reading vulnerability, allowing remote attackers with regular privileges to exploit Absolute Path Traversal to download arbitrary system files.	6.5	More Details
CVE-2025-57887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster allows Stored XSS. This issue affects Jobmonster: from n/a through 4.8.0.	6.5	More Details
CVE-2025-8678	The WP Crontrol plugin for WordPress is vulnerable to Server-Side Request Forgery in versions 1.17.0 to 1.19.1 via the 'wp_remote_request' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	6.5	More Details
CVE-2025-9257	WebITR developed by Uniong has an Arbitrary File Reading vulnerability, allowing remote attackers with regular privileges to exploit Absolute Path Traversal to download arbitrary system files.	6.5	More Details

CVE-2025-55621	An Insecure Direct Object Reference (IDOR) vulnerability in Reolink v4.54.0.4.20250526 allows unauthorized attackers to access and download other users' profile photos via a crafted URL.	6.5	More Details
CVE-2025-49422	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aelora iframe Wrapper allows DOM-Based XSS. This issue affects iframe Wrapper: from n/a through 0.1.1.	6.5	More Details
CVE-2025-53993	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetPopup allows Retrieve Embedded Sensitive Data. This issue affects JetPopup: from n/a through 2.0.15.	6.5	More Details
CVE-2025-53992	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetTricks allows Retrieve Embedded Sensitive Data. This issue affects JetTricks: from n/a through 1.5.4.1.	6.5	More Details
CVE-2025-53988	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetBlocks For Elementor allows Retrieve Embedded Sensitive Data. This issue affects JetBlocks For Elementor: from n/a through 1.3.18.	6.5	More Details
CVE-2025-53987	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetMenu allows Retrieve Embedded Sensitive Data. This issue affects JetMenu: from n/a through 2.4.11.1.	6.5	More Details
CVE-2025-53985	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetTabs allows Retrieve Embedded Sensitive Data. This issue affects JetTabs: from n/a through 2.2.9.	6.5	More Details
CVE-2025-53983	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetElements For Elementor allows Retrieve Embedded Sensitive Data. This issue affects JetElements For Elementor: from n/a through 2.7.7.	6.5	More Details
CVE-2025-53561	Path Traversal vulnerability in miniOrange Prevent files / folders access allows Path Traversal. This issue affects Prevent files / folders access: from n/a through 2.6.0.	6.5	More Details
CVE-2025-53196	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetEngine allows Retrieve Embedded Sensitive Data. This issue affects JetEngine: from n/a through 3.7.0.	6.5	More Details
CVE-2025-53195	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine allows Stored XSS. This issue affects JetEngine: from n/a through 3.7.0.	6.5	More Details
CVE-2025-49893	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in liseperu Elizaibots allows Stored XSS. This issue affects Elizaibots: from n/a through 1.0.2.	6.5	More Details
CVE-2025-49436	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in thiudis Custom Menu allows Stored XSS. This issue affects Custom Menu: from n/a through 1.8.	6.5	More Details
CVE-2025-49424	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in diego.benna Essential Doo Components for Visual Composer allows DOM-Based XSS. This issue affects Essential Doo Components for Visual Composer: from n/a through 1.9.	6.5	More Details
CVE-2025-49420	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pierre-Henri Lavigne Markup Markdown allows Stored XSS. This issue affects Markup Markdown: from n/a through 3.20.6.	6.5	More Details
CVE-2025-54008	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetSmartFilters allows Retrieve Embedded Sensitive Data. This issue affects JetSmartFilters: from n/a through 3.6.7.	6.5	More Details
CVE-2025-49411	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vikas Sharma iFrame Block allows Stored XSS. This issue affects iFrame Block: from n/a through 0.1.1.	6.5	More Details
CVE-2025-49410	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imran Emu TC Testimonials allows Stored XSS. This issue affects TC Testimonials: from n/a through 1.1.1.	6.5	More Details
CVE-2025-48108	Missing Authorization vulnerability in Mojoomla School Management allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects School Management: from n/a through 93.2.0.	6.5	More Details
CVE-2025-49400	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in osama.esh WP Visitor Statistics (Real Time Traffic) allows Stored XSS. This issue affects WP Visitor Statistics (Real Time Traffic): from n/a through 8.2.	6.5	More Details
CVE-2025-49397	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Colorbox Lightbox allows Stored XSS. This issue affects Colorbox Lightbox: from n/a through 1.1.5.	6.5	More Details
CVE-2025-49395	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Icons allows Stored XSS. This issue affects Themify Icons: from n/a through 2.0.3.	6.5	More Details

CVE-2025-49389	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WEN Solutions Notice Bar allows Stored XSS. This issue affects Notice Bar: from n/a through 3.1.3.	6.5	More Details
CVE-2025-47650	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Infility Infility Global allows Path Traversal. This issue affects Infility Global: from n/a through 2.14.7.	6.5	More Details
CVE-2025-25732	Incorrect access control in the EEPROM component of Kapsch TrafficCom RIS-9160 & RIS-9260 Roadside Units (RSUs) v3.2.0.829.23, v3.8.0.1119.42, and v4.6.0.1211.28 allows attackers to replace password hashes stored in the EEPROM with hashes of their own, leading to the escalation of privileges to root.	6.5	More Details
CVE-2025-52219	SelectZero SelectZero Data Observability Platform before 2025.5.2 contains an Open Redirect vulnerability. Legacy UI fields can be used to create arbitrary external links via HTML Injection.	6.5	More Details
CVE-2025-57791	An issue was discovered in Commvault before 11.36.60. A security vulnerability has been identified that allows remote attackers to inject or manipulate command-line arguments passed to internal components due to insufficient input validation. Successful exploitation results in a valid user session for a low privilege role.	6.5	More Details
CVE-2025-57788	An issue was discovered in Commvault before 11.36.60. A vulnerability in a known login mechanism allows unauthenticated attackers to execute API calls without requiring user credentials. RBAC helps limit the exposure but does not eliminate risk.	6.5	More Details
CVE-2025-53998	Insertion of Sensitive Information Into Sent Data vulnerability in Crocoblock JetWooBuilder allows Retrieve Embedded Sensitive Data. This issue affects JetWooBuilder: from n/a through 2.1.20.	6.5	More Details
CVE-2025-54019	Improper Control of Generation of Code ('Code Injection') vulnerability in Bearsthemes Alone allows Code Injection. This issue affects Alone: from n/a through n/a.	6.5	More Details
CVE-2025-55622	Reolink v4.54.0.4.20250526 was discovered to contain a task hijacking vulnerability due to inappropriate taskAffinity settings.	6.5	More Details
CVE-2025-44178	DASAN GPON ONU H660WM H660WMR210825 is susceptible to improper access control under its default settings. Attackers can exploit this vulnerability to gain unauthorized access to sensitive information and modify its configuration via the UPnP protocol WAN sides without any authentication.	6.5	More Details
CVE-2025-55625	An open redirect vulnerability in Reolink v4.54.0.4.20250526 allows attackers to redirect users to a malicious site via a crafted URL.	6.5	More Details
CVE-2025-55629	Insecure permissions in Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 allow attackers to arbitrarily change other users' passwords via manipulation of the userName value.	6.5	More Details
CVE-2025-57749	n8n is a workflow automation platform. Before 1.106.0, a symlink traversal vulnerability was discovered in the Read/Write File node in n8n. While the node attempts to restrict access to sensitive directories and files, it does not properly account for symbolic links (symlinks). An attacker with the ability to create symlinks—such as by using the Execute Command node—could exploit this to bypass the intended directory restrictions and read from or write to otherwise inaccessible paths. Users of n8n.cloud are not impacted. Affected users should update to version 1.106.0 or later.	6.5	More Details
CVE-2025-55637	Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 was discovered to contain a command injection vulnerability via the setddns_pip_system() function.	6.5	More Details
CVE-2022-45133	Mahara 21.10 before 21.10.6, 22.04 before 22.04.4, and 22.10 before 22.10.1 allows unsafe font upload for skins. A particularly structured XML file could allow one to traverse the server to obtain access to secure files or cause code execution based on the payload.	6.5	More Details
CVE-2025-20269	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, low-privileged, remote attacker to retrieve arbitrary files from the underlying file system on an affected device. This vulnerability is due to insufficient input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface on an affected device. A successful exploit could allow the attacker to access sensitive files from the affected device.	6.5	More Details
CVE-2025-8562	The Custom Query Shortcode plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 0.4.0 via the 'lens' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of files on the server, which can contain sensitive information.	6.5	More Details
CVE-2024-46412	Incorrect access control in the prehandle function of Rebuild v3.7.7 allows attackers to bypass authentication via a crafted GET request sent to /commons/ip-location.	6.5	More Details
CVE-2025-54025	Missing Authorization vulnerability in Elliot Sowersby / RelyWP Coupon Affiliates allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Coupon Affiliates: from n/a through 6.4.0.	6.5	More Details
CVE-2025-29524	Incorrect access control in the component /cgi-bin/system_diagnostic_main.asp of DASAN GPON ONU H660WM H660WMR210825 allows attackers to access sensitive information.	6.5	More Details
CVE-2025-29522	D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the ping function.	6.5	More Details

CVE-2025-50864	An Origin Validation Error in the elysia-cors library thru 1.3.0 allows attackers to bypass Cross-Origin Resource Sharing (CORS) restrictions. The library incorrectly validates the supplied origin by checking if it is a substring of any domain in the site's CORS policy, rather than performing an exact match. For example, a malicious origin like "notexample.com", "example.common.net" is whitelisted when the site's CORS policy specifies "example.com." This vulnerability enables unauthorized access to user data on sites using the elysia-cors library for CORS validation.	6.5	More Details
CVE-2025-44179	Hitron CGNF-TWN 3.1.1.43-TWN-pre3 contains a command injection vulnerability in the telnet service. The issue arises due to improper input validation within the telnet command handling mechanism. An attacker can exploit this vulnerability by injecting arbitrary commands through the telnet interface when prompted for inputs or commands. Successful exploitation could lead to remote code execution (RCE) under the privileges of the telnet user, potentially allowing unauthorized access to system settings and sensitive information.	6.5	More Details
CVE-2025-36114	IBM QRadar SOAR Plugin App 1.0.0 through 5.6.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	6.5	More Details
CVE-2025-55499	Tenda AC6 V15.03.06.23_multi was discovered to contain a buffer overflow via the ntpServer parameter in the fromSetSysTime function.	6.5	More Details
CVE-2025-56215	phpgurukul Hospital Management System 4.0 is vulnerable to SQL Injection in contact.php via the pagetitle parameter.	6.5	More Details
CVE-2025-7777	The mirror-registry doesn't properly sanitize the host header HTTP header in HTTP request received, allowing an attacker to perform malicious redirects to attacker-controlled domains or phishing campaigns.	6.5	More Details
CVE-2025-57729	In JetBrains IntelliJ IDEA before 2025.2 unexpected plugin startup was possible due to automatic LSP server start	6.5	More Details
CVE-2025-57728	In JetBrains IntelliJ IDEA before 2025.2 improper access control allowed Code With Me guest to discover hidden files	6.5	More Details
CVE-2025-54046	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuanticaLabs Cost Calculator allows Stored XSS. This issue affects Cost Calculator: from n/a through 7.4.	6.5	More Details
CVE-2025-54040	Missing Authorization vulnerability in Webba Appointment Booking Webba Booking allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Webba Booking: from n/a through 5.1.20.	6.5	More Details
CVE-2025-55522	Cross-site scripting (XSS) vulnerability in the component /common/reports of Akaunting v3.1.18 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name parameter.	6.5	More Details
CVE-2025-9382	A weakness has been identified in FNKvision Y215 CCTV Camera 10.194.120.40. This vulnerability affects unknown code of the file s1_rf_test_config of the component Telnet Sevice. Executing manipulation can lead to backdoor. The physical device can be targeted for the attack. This attack is characterized by high complexity. It is stated that the exploitability is difficult. 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.	6.4	More Details
CVE-2025-8208	The Spexo Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.0.23 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-2025-9131	The Ogulo – 360° Tour plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘slug’ parameter in all versions up to, and including, 1.0.11 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-2025-8062	The WS Theme Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ws_weather shortcode in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7957	The ShortcodeHub plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘author_link_target’ parameter in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9277	The SiteSEO – SEO Simplified plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the broken preg_replace expression in all versions up to, and including, 1.2.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8064	The Bible SuperSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘selector_height’ parameter in all versions up to, and including, 6.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8607	The SlingBlocks – Gutenberg Blocks by FunnelKit (Formerly WooFunnels) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown block's attributes in all versions up to, and including, 1.6.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
	The WPC Smart Quick View for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's woosq_btn		

CVE-2025-8618	shortcode in all versions up to, and including, 4.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9411	A security vulnerability has been detected in lostvip-com ruoyi-go up to 2.1. The impacted element is the function SelectPageList of the file modules/system/service/LoginInforService.go. The manipulation of the argument isAsc leads to sql injection. 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.	6.3	More Details
CVE-2024-39954	CWE-918 Server-Side Request Forgery (SSRF) in eventmesh-runtime module in WebhookUtil.java on windows\linux\mac os e.g. allows the attacker can abuse functionality on the server to read or update internal resources. Users are recommended to upgrade to version 1.12.0 or use the master branch , which fixes this issue.	6.3	More Details
CVE-2025-9417	A weakness has been identified in itsourcecode Apartment Management System 1.0. This issue affects some unknown processing of the file /employee/addemployee.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-27714	An attacker could exploit this vulnerability by uploading arbitrary files via the a specific endpoint, leading to unauthorized remote code execution or system compromise.	6.3	More Details
CVE-2025-24489	An attacker could exploit this vulnerability by uploading arbitrary files via a specific service, which could lead to system compromise.	6.3	More Details
CVE-2025-9415	A vulnerability was identified in GreenCMS up to 2.3.0603. This affects an unknown part of the file /index.php?m=admin&c=media&a=fileconnect. The manipulation of the argument upload[] leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-9413	A flaw has been found in lostvip-com ruoyi-go up to 2.1. This impacts the function SelectListByPage of the file modules/system/system_router.go. This manipulation of the argument orderByColumn/isAsc causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9412	A vulnerability was detected in lostvip-com ruoyi-go up to 2.1. This affects the function SelectListByPage of the file modules/system/dao/DictDataDao.go. The manipulation of the argument orderByColumn/isAsc results in sql injection. 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-2025-9410	A weakness has been identified in lostvip-com ruoyi-go up to 2.1. The affected element is the function SelectListByPage of the file modules/system/dao/GenTableDao.go. Executing manipulation of the argument isAsc/orderByColumn 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. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9406	A weakness has been identified in xuhuisheng lemon up to 1.13.0. This affects the function uploadImage of the file CmsArticleController.java of the component com.mossle.cms.web.CmsArticleController.uploadImage. This manipulation of the argument Upload causes unrestricted upload. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-9400	A flaw has been found in YiFang CMS up to 2.0.5. This affects the function mergeMultipartUpload of the file app/utils/base/plugin/P_file.php. This manipulation of the argument File causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9399	A vulnerability was detected in YiFang CMS up to 2.0.5. Affected by this issue is some unknown functionality of the file app/logic/L_tool.php. The manipulation of the argument new_url results in sql injection. The attack may 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-2025-9244	A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This vulnerability affects the function addStaticRoute of the file /goform/addStaticRoute. Such manipulation of the argument staticRoute_IP_setting/staticRoute_Netmask_setting/staticRoute_Gateway_setting/staticRoute_Metric_setting/staticRoute_destType_setting leads to os command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9397	A weakness has been identified in givanz Vvveb up to 1.0.7.2. Affected is an unknown function of the file /system/traits/media.php. Executing manipulation of the argument files[] can lead to unrestricted upload. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. Applying a patch is advised to resolve this issue. The code maintainer explains, that "[he] fixed the code to remove this vulnerability and will make a new release".	6.3	More Details
CVE-2025-9395	A vulnerability was identified in wangsongyan wblog 0.0.1. This affects the function RestorePost of the file backup.go. Such manipulation of the argument fileName leads to server-side request forgery. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9241	A weakness has been identified in elunez eladmin up to 2.7. This affects the function exportUser. This manipulation causes csv injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-9391	A weakness has been identified in Bjskzy Zhiyou ERP up to 11.0. Affected by this issue is the function getFieldValue of the component com.artery.workflow.ServiceImpl. This manipulation of the argument sql causes sql injection. 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-	A vulnerability was found in DCN DCME-720 9.1.5.11. This affects an unknown function of the file /usr/local/www/function/audit/newstatistics/ip_block.php of the component Web Management Backend. Performing manipulation of the argument ip results in os command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be	6.3	More Details

9387	used. Other products might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-9236	A vulnerability has been found in Portabilis i-Diario up to 2.10. This affects an unknown function of the file /intranet/educar_tipo_usuario_lst.php of the component Tipos de usàrio Page. Such manipulation of the argument nm_tipo leads to sql injection. The attack may be performed from a remote location. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-9362	A flaw has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. The impacted element is the function urlFilterManageRule of the file /goform/urlFilterManageRule. Executing manipulation of the argument urlFilterRuleName/scheduleUrl/addURLFilter can lead to stack-based buffer overflow. The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-57818	Firecrawl turns entire websites into LLM-ready markdown or structured data. Prior to version 2.0.1, a server-side request forgery (SSRF) vulnerability was discovered in Firecrawl's webhook functionality. Authenticated users could configure a webhook to an internal URL and send POST requests with arbitrary headers, which may have allowed access to internal systems. This has been fixed in version 2.0.1. If upgrading is not possible, it is recommend to isolate Firecrawl from any sensitive internal systems.	6.3	More Details
CVE-2025-9173	A weakness has been identified in Emlog Pro up to 2.5.18. This issue affects some unknown processing of the file /admin/media.php?action=upload&sid=0. Executing manipulation of the argument File can lead to unrestricted upload. The attack may be launched 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-2024-39923	An issue was discovered in Mahara 24.04 before 24.04.2 and 23.04 before 23.04.7. The About, Contact, and Help footer links can be set up to be vulnerable to Cross Site Scripting (XSS) due to not sanitising the values. These links can only be set up by an admin but are clickable by any logged-in person.	6.1	More Details
CVE-2025-50733	NextChat contains a cross-site scripting (XSS) vulnerability in the HTMLPreview component of artifacts.tsx that allows attackers to execute arbitrary JavaScript code when HTML content is rendered in the AI chat interface. The vulnerability occurs because user-influenced HTML from AI responses is rendered in an iframe with 'allow-scripts' sandbox permission without proper sanitization. This can be exploited through specifically crafted prompts that cause the AI to generate malicious HTML/JavaScript code. When a user views the HTML preview, the injected JavaScript executes in the user's browser context, potentially allowing attackers to exfiltrate sensitive information (including API keys stored in localStorage), perform actions on behalf of the user, and steal session data.	6.1	More Details
CVE-2025-1139	IBM Edge Application Manager 4.5 could allow a local user to read or modify resources that they should not have authorization to access due to incorrect permission assignment.	6.1	More Details
CVE-2025-55574	Cross Site Scripting vulnerability in docmost v.0.21.0 and before allows an attacker to execute arbitrary code	6.1	More Details
CVE-2025-50858	Reflected Cross-Site Scripting in the List MySQL Databases function in Easy Hosting Control Panel (EHCP) 20.04.1.b allows authenticated attackers to execute arbitrary JavaScript via the action parameter.	6.1	More Details
CVE-2025-57762	WeGIA is a Web manager for charitable institutions. Prior to 3.4.7, there is a Stored Cross-Site Scripting (XSS) vulnerability in the dependente_docdependente.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the nome parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. This vulnerability is fixed in 3.4.7.	6.1	More Details
CVE-2025-50859	Reflected Cross-Site Scripting in the Change Template function in Easy Hosting Control Panel (EHCP) 20.04.1.b allows authenticated attackers to execute arbitrary JavaScript via the template parameter.	6.1	More Details
CVE-2024-45753	In Mahara 23.04.8 and 24.04.4, the external RSS feed block can cause XSS if the external feed XML has a malicious value for the link attribute.	6.1	More Details
CVE-2025-57763	WeGIA is a Web manager for charitable institutions. Prior to 3.4.7, there is a Reflected Cross-Site Scripting (XSS) vulnerability in the insere_despacho.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the cpf sccs. This vulnerability is fixed in 3.4.7.	6.1	More Details
CVE-2025-44002	Race Condition in the Directory Validation Logic in the TeamViewer Full Client and Host prior version 15.69 on Windows allows a local non-admin user to create arbitrary files with SYSTEM privileges, potentially leading to a denial-of-service condition, via symbolic link manipulation during directory verification.	6.1	More Details
CVE-2025-52035	A vulnerability in NotesCMS and specifically in the page /index.php?route=notes. The manipulation of the title of the service descriptions leads to a stored XSS vulnerability. The issue was confirmed to be present in the source code as of commit 7d821a0f028b0778b245b99ab3d3bff1ac10e2d3 (dated 2024-05-08) and was fixed in commit 95322c5121dbd7070f3bd54f2848079654a0a8ea (dated 2025-03-31). The attack can be launched remotely.	6.1	More Details
CVE-2025-52036	A vulnerability has been found in NotesCMS and classified as medium. Affected by this vulnerability is the page /index.php?route=categories. The manipulation of the title of the service descriptions leads to a stored XSS vulnerability. The issue was confirmed to be present in the source code as of commit 7d821a0f028b0778b245b99ab3d3bff1ac10e2d3 (dated 2024-05-08), and was fixed in commit 95322c5121dbd7070f3bd54f2848079654a0a8ea (dated 2025-03-31). The attack can be launched remotely. CWE Definition of the Vulnerability: CWE-79.	6.1	More Details
CVE-2025-52037	A vulnerability has been found in NotesCMS and classified as medium. Affected by this vulnerability is the page /index.php?route=sites. The manipulation of the title of the service descriptions leads to a stored XSS vulnerability. The issue was confirmed to be present in the source code as of commit 7d821a0f028b0778b245b99ab3d3bff1ac10e2d3 (dated 2024-05-08), and was fixed in commit 95322c5121dbd7070f3bd54f2848079654a0a8ea (dated 2025-03-31). The attack can be launched remotely. CWE Definition of the Vulnerability: CWE-79.	6.1	More Details
CVE-2025-56432	A cross-site scripting (XSS) vulnerability exists in Nagios XI 2024R2. The vulnerability allows remote attackers to execute arbitrary JavaScript in the context of a logged-in user's session via a specially crafted URL. The issue resides in a web component responsible for rendering performance-related data.	6.1	More Details

CVE-2025-1494	IBM Cognos Command Center 10.2.4.1 and 10.2.5 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim.	6.1	More Details
CVE-2025-55620	A cross-site scripting (XSS) vulnerability in the valuateJavascript() function of Reolink v4.54.0.4.20250526 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2025-49889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in imaprogrammer Custom Comment allows Stored XSS. This issue affects Custom Comment: from n/a through 2.1.6.	5.9	More Details
CVE-2025-49434	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stijnvanderree Laposta WooCommerce allows Stored XSS. This issue affects Laposta WooCommerce: from n/a through 1.9.1.	5.9	More Details
CVE-2025-8415	A vulnerability was found in the Cryostat HTTP API. Cryostat's HTTP API binds to all network interfaces, allowing possible external visibility and access to the API port if Network Policies are disabled, allowing an unauthenticated, malicious attacker to jeopardize the environment.	5.9	More Details
CVE-2025-49894	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rewish WP Emmet allows Stored XSS. This issue affects WP Emmet: from n/a through 0.3.4.	5.9	More Details
CVE-2025-49892	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in badasswp Pending Order Bot allows Stored XSS. This issue affects Pending Order Bot: from n/a through 1.0.2.	5.9	More Details
CVE-2025-57891	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpecommerce Recurring PayPal Donations allows Stored XSS. This issue affects Recurring PayPal Donations: from n/a through 1.8.	5.9	More Details
CVE-2025-49891	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in riotweb Contact Info Widget allows Stored XSS. This issue affects Contact Info Widget: from n/a through 2.6.2.	5.9	More Details
CVE-2025-57813	traQ is a messenger application built for Digital Creators Club traP. Prior to version 3.25.0, a vulnerability exists where sensitive information, such as OAuth tokens, are recorded in log files when an error occurs during the execution of an SQL query. An attacker could intentionally trigger an SQL error by methods such as placing a high load on the database. This could allow an attacker who has the authority to view the log files to illicitly acquire the recorded sensitive information. This vulnerability has been patched in version 3.25.0. If upgrading is not possible, a temporary workaround involves reviewing access permissions for SQL error logs and strictly limiting access to prevent unauthorized users from viewing them.	5.9	More Details
CVE-2025-49409	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brewlabs SensorPress allows Stored XSS. This issue affects SensorPress: from n/a through 1.0.	5.9	More Details
CVE-2025-57890	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pierre Lannoy Sessions allows Stored XSS. This issue affects Sessions: from n/a through 3.2.0.	5.9	More Details
CVE-2025-35113	Agiloft Release 28 does not properly neutralize special elements used in an EUI template engine, allowing an authenticated attacker to achieve remote code execution by loading a specially crafted payload. Users should upgrade to Agiloft Release 31.	5.9	More Details
CVE-2025-49412	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in numixtech Page Transition allows Stored XSS. This issue affects Page Transition: from n/a through 1.3.	5.9	More Details
CVE-2025-49392	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Audio Dock allows Stored XSS. This issue affects Themify Audio Dock: from n/a through 2.0.5.	5.9	More Details
CVE-2025-49890	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jorge Garcia de Bustos AWStats Script allows Stored XSS. This issue affects AWStats Script: from n/a through 0.3.	5.9	More Details
CVE-2025-49428	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dourou Cookie Warning allows Stored XSS. This issue affects Cookie Warning: from n/a through 1.3.	5.9	More Details
CVE-2025-49413	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wishloop Terms of Service & Privacy Policy Generator allows Stored XSS. This issue affects Terms of Service & Privacy Policy Generator: from n/a through 1.0.	5.9	More Details
CVE-2025-4437	There's a vulnerability in the CRI-O application where when container is launched with securityContext.runAsUser specifying a non-existent user, CRI-O attempts to create the user, reading the container's entire /etc/passwd file into memory. If this file is excessively large, it can cause the a high memory consumption leading applications to be killed due to out-of-memory. As a result a denial-of-service can be achieved, possibly disrupting other pods and services running in the same host.	5.7	More Details
CVE-2025-9262	A flaw has been found in wong2 mcp-cli 1.13.0. Affected is the function redirectToAuthorization of the file /src/oauth/provider.js of the component oAuth Handler. This manipulation causes os command injection. The attack may be initiated remotely. The attack is considered to have high complexity. The exploitability is told to be difficult. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2025-	Stored cross-site scripting (XSS) in the web interface of MiR software versions prior to 3.0.0 on MiR Robots and MiR Fleet allows execution of arbitrary JavaScript code in a victim’s browser	5.5	More Details

9225			
CVE-2025-57733	In JetBrains TeamCity before 2025.07.1 sMTP injection was possible allowing modification of email content	5.5	More Details
CVE-2025-57704	Delta Electronics EIP Builder version 1.11 is vulnerable to a File Parsing XML External Entity Processing Information Disclosure Vulnerability.	5.5	More Details
CVE-2025-55623	An issue in the lock screen component of Reolink v4.54.0.4.20250526 allows attackers to bypass authentication via using an ADB (Android Debug Bridge).	5.4	More Details
CVE-2025-51818	MCCMS 2.7.0 is vulnerable to Arbitrary file deletion in the Backups.php component. This allows an attacker to execute arbitrary commands	5.4	More Details
CVE-2025-54812	Improper Output Neutralization for Logs vulnerability in Apache Log4cxx. When using HTMLLayout, logger names are not properly escaped when writing out to the HTML file. If untrusted data is used to retrieve the name of a logger, an attacker could theoretically inject HTML or Javascript in order to hide information from logs or steal data from the user. In order to activate this, the following sequence must occur: * Log4cxx is configured to use HTMLLayout. * Logger name comes from an untrusted string * Logger with compromised name logs a message * User opens the generated HTML log file in their browser, leading to potential XSS Because logger names are generally constant strings, we assess the impact to users as LOW This issue affects Apache Log4cxx: before 1.5.0. Users are recommended to upgrade to version 1.5.0, which fixes the issue.	5.4	More Details
CVE-2025-47054	Adobe Experience Manager versions 6.5.22 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. A low privileged attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a specially crafted web page.	5.4	More Details
CVE-2025-46998	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-46962	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-46936	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-46932	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-46856	Adobe Experience Manager versions 6.5.22 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. A low privileged attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a specially crafted web page.	5.4	More Details
CVE-2025-52130	File upload vulnerability in WebErpMesv2 1.17 in the app/Http/Controllers/FactoryController.php controller. This flaw allows an authenticated attacker to upload arbitrary files, including PHP scripts, which can be accessed via direct GET requests, potentially resulting in remote code execution (RCE) on the web server.	5.4	More Details
CVE-2025-8102	The Easy Digital Downloads plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.5.0. This is due to missing nonce validations in the edd_sendwp_disconnect() and edd_sendwp_remote_install() functions. This makes it possible for unauthenticated attackers to deactivate or download and activate the SendWP plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2025-1142	IBM Edge Application Manager 4.5 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2025-57886	Authorization Bypass Through User-Controlled Key vulnerability in Equalize Digital Accessibility Checker by Equalize Digital allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accessibility Checker by Equalize Digital: from n/a through 1.30.0.	5.4	More Details
CVE-2025-46849	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2025-57789	An issue was discovered in Commvault before 11.36.60. During the brief window between installation and the first administrator login, remote attackers may exploit the default credential to gain admin control. This is limited to the setup phase, before any jobs have been configured.	5.4	More Details
CVE-2025-36042	IBM QRadar SIEM 7.5 through 7.5.0 Dashboard is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2025-9264	A vulnerability was found in Xuxueli xxl-job up to 3.1.1. Affected by this issue is the function remove of the file /src/main/java/com/xxl/job/admin/controller/JobInfoController.java of the component Jobs Handler. Performing manipulation of the argument ID results in improper control of resource identifiers. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	5.4	More Details
CVE-2025-46852	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE-2025-55627	Insufficient privilege verification in Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 allows authenticated attackers to create accounts with elevated privileges.	5.3	More Details
CVE-2025-55624	An intent redirection vulnerability in Reolink v4.54.0.4.20250526 allows unauthorized attackers to access internal functions or access non-public components.	5.3	More Details
CVE-2025-57770	The open-source identity infrastructure software Zitadel allows administrators to disable the user self-registration. Versions 4.0.0 to 4.0.2, 3.0.0 to 3.3.6, and all versions prior to 2.71.15 are vulnerable to a username enumeration issue in the login interface. The login UI includes a security feature, Ignoring unknown usernames, that is intended to prevent username enumeration by returning a generic response for both valid and invalid usernames. This vulnerability allows an unauthenticated attacker to bypass this protection by submitting arbitrary userIDs to the select account page and distinguishing between valid and invalid accounts based on the system's response. For effective exploitation, an attacker needs to iterate through possible userIDs, but the impact can be limited by implementing rate limiting or similar measures. The issue has been patched in versions 4.0.3, 3.4.0, and 2.71.15.	5.3	More Details
CVE-2025-55626	An Insecure Direct Object Reference (IDOR) vulnerability in Reolink Smart 2K+ Plug-in Wi-Fi Video Doorbell with Chime - firmware v3.0.0.4662_2503122283 allows unauthorized attackers to access the Admin-only settings and edit the session storage.	5.3	More Details
CVE-2025-29521	Insecure default credentials for the Adminsitrator account of D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 allows attackers to escalate privileges via a bruteforce attack.	5.3	More Details
CVE-2025-7821	The WC Plus plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'pluswc_logo_favicon_logo_base' AJAX action in all versions up to, and including, 1.2.0. This makes it possible for unauthenticated attackers to update the site's favicon logo base.	5.3	More Details
CVE-2025-9385	A flaw has been found in appneta tcpreplay up to 4.5.1. The affected element is the function fix_ipv6_checksums of the file edit_packet.c of the component tcprewrite. This manipulation causes use after free. The attack is restricted to local execution. The exploit has been published and may be used. Upgrading to version 4.5.2-beta3 is sufficient to fix this issue. It is advisable to upgrade the affected component.	5.3	More Details
CVE-2025-9386	A vulnerability has been found in appneta tcpreplay up to 4.5.1. The impacted element is the function get_l2len_protocol of the file get.c of the component tcprewrite. Such manipulation leads to use after free. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. Upgrading to version 4.5.2-beta3 is sufficient to resolve this issue. You should upgrade the affected component.	5.3	More Details
CVE-2025-9390	A security flaw has been discovered in vim up to 9.1.1615. Affected by this vulnerability is the function main of the file src/xxd/xxd.c of the component xxd. The manipulation results in buffer overflow. The attack requires a local approach. The exploit has been released to the public and may be exploited. Upgrading to version 9.1.1616 addresses this issue. The patch is identified as eeef7c77436a78cd27047b0f5fa6925d56de3cb0. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2025-9394	A flaw has been found in PoDoFo 1.1.0-dev. This issue affects the function PdfTokenizer::DetermineDataType of the file src/podofo/main/PdfTokenizer.cpp of the component PDF Dictionary Parser. Executing manipulation can lead to use after free. It is possible to launch the attack on the local host. The exploit has been published and may be used. This patch is called 22d16cb142f293bf956f66a4d399cdd65576d36c. A patch should be applied to remediate this issue.	5.3	More Details
CVE-2025-9398	A security vulnerability has been detected in YiFang CMS up to 2.0.5. Affected by this vulnerability is the function exportInstallTable of the file app/utils/base/database/Migrate.php. The manipulation leads to information disclosure. The attack may 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.	5.3	More Details
CVE-2025-9405	A security flaw has been discovered in Open5GS up to 2.7.5. The impacted element is the function gmm_state_exception of the file src/amf/gmm-sm.c. The manipulation results in reachable assertion. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited. The patch is identified as 8e5fed16114f2f5e40bee1b161914b592b2b7b8f. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-2025-5514	Improper Handling of Length Parameter Inconsistency vulnerability in web server function on Mitsubishi Electric Corporation MELSEC iQ-F Series CPU module allows a remote unauthenticated attacker to delay the processing of the web server function and prevent legitimate users from utilizing the web server function, by sending a specially crafted HTTP request.	5.3	More Details
CVE-2025-29519	A command injection vulnerability in the EXE parameter of D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 allows attackers to execute arbitrary commands via supplying a crafted GET request.	5.3	More Details
CVE-2025-29520	Incorrect access control in the Maintenance module of D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 allows authenticated attackers with low-level privileges to arbitrarily change the high-privileged account passwords and escalate privileges.	5.3	More Details
CVE-2025-29525	DASAN GPON ONU H660WM OS version H660WMR210825 Hardware version DS-E5-583-A1 was discovered to contain insecure default credentials in the modem's control panel.	5.3	More Details
CVE-2025-9229	Information disclosure vulnerability in error handling in MiR software prior to version 3.0.0 allows unauthenticated attackers to view detailed error information, such as file paths and other data, via access to verbose error pages.	5.3	More Details
CVE-2025-49406	Missing Authorization vulnerability in favethemes Houzez allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Houzez: from n/a through 4.1.1.	5.3	More Details
CVE-2025-25733	Incorrect access control in the SPI Flash Chip of Kapsch TrafficCom RIS-9160 & RIS-9260 Roadside Units (RSUs) v3.2.0.829.23, v3.8.0.1119.42, and v4.6.0.1211.28 allows physically proximate attackers to arbitrarily modify SPI flash regions, leading to a degradation of the security posture of the device.	5.3	More Details
CVE-2025-	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in ProveSource LTD ProveSource Social Proof	5.3	More

48355	allows Retrieve Embedded Sensitive Data.This issue affects ProveSource Social Proof: from n/a through 3.0.5.		Details
CVE-2025-9176	A security flaw has been discovered in neurobin shc up to 4.0.3. Impacted is the function make of the file src/shc.c of the component Environment Variable Handler. The manipulation results in os command injection. The attack is only possible with local access. The exploit has been released to the public and may be exploited.	5.3	More Details
CVE-2025-9310	A vulnerability was determined in yeqifu carRental up to 3fabb7eae93d2094266388639803 01d6f99866b3. Affected by this vulnerability is an unknown functionality of the file /carRental_war/druid/login.html of the component Druid. Executing manipulation can lead to hard-coded credentials. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	5.3	More Details
CVE-2025-55229	Improper verification of cryptographic signature in Windows Certificates allows an unauthorized attacker to perform spoofing over a network.	5.3	More Details
CVE-2025-55366	Incorrect access control in the component \controller\UserController.java of jshERP v3.5 allows attackers to arbitrarily reset user account passwords and execute a horizontal privilege escalation attack.	5.3	More Details
CVE-2025-55367	Incorrect access control in the component \controller\SupplierController.java of jshERP v3.5 allows unauthorized attackers to arbitrarily modify the supplier status under any account.	5.3	More Details
CVE-2025-55371	Incorrect access control in the component /controller/PersonController.java of jshERP v3.5 allows unauthorized attackers to obtain all the information of the handler by executing the getAllList method.	5.3	More Details
CVE-2025-47184	An XML external entities (XXE) injection vulnerability in the /init API endpoint in Exagid EX10 before 6.4.0 P20, 7.0.1 P12, and 7.2.0 P08 allows an authenticated, unprivileged attacker to achieve information disclosure and privilege escalation via a crafted ISys XML message.	5.3	More Details
CVE-2025-50691	MCSManager 10.5.3 daemon process runs as a root account by default, and its sensitive data (including tokens and terminal content) is stored in the data directory, readable by all users. Other users on the system can read the daemon's key and use it to log in, leading to privilege escalation.	5.3	More Details
CVE-2025-57896	Missing Authorization vulnerability in andy_moyle Church Admin allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Church Admin: from n/a through 5.0.26.	5.3	More Details
CVE-2025-38742	Dell iDRAC Service Module (iSM), versions prior to 6.0.3.0, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	5.3	More Details
CVE-2025-9300	A vulnerability was found in saitoha libsixel up to 1.10.3. Affected by this issue is the function sixel_debug_print_palette of the file src/encoder.c of the component img2sixel. The manipulation results in stack-based buffer overflow. The attack must be initiated from a local position. The exploit has been made public and could be used. The patch is identified as 316c086e79d66b62c0c4bc66229ee894e4fdb7d1. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-2025-57888	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in NooTheme Jobmonster allows Retrieve Embedded Sensitive Data. This issue affects Jobmonster: from n/a through 4.8.0.	5.3	More Details
CVE-2025-57730	In JetBrains IntelliJ IDEA before 2025.2 hTML injection was possible via Remote Development feature	5.2	More Details
CVE-2024-46413	Rebuild v3.7.7 was discovered to contain a Server-Side Request Forgery (SSRF) via the type parameter in the com.rebuild.web.admin.rbstore.RBStoreController#loadDataIndex method.	5.1	More Details
CVE-2025-27213	An Improper Access Control could allow a malicious actor authenticated in the API of certain UniFi Connect devices to enable Android Debug Bridge (ADB) and make unsupported changes to the system. Affected Products: UniFi Connect EV Station Pro (Version 1.5.18 and earlier) UniFi Connect Display (Version 1.9.324 and earlier) UniFi Connect Display Cast (Version 1.9.301 and earlier) UniFi Connect Display Cast Pro (Version 1.0.78 and earlier) UniFi Connect Display Cast Lite (Version 1.0.3 and earlier) Mitigation: Update UniFi Connect EV Station Pro to Version 1.5.27 or later Update UniFi Connect Display to Version 1.13.6 or later Update UniFi Connect Display Cast to Version 1.10.3 or later Update UniFi Connect Display Cast Pro to Version 1.0.83 or later Update UniFi Connect Display Cast Lite to Version 1.1.3 or later	4.9	More Details
CVE-2025-20131	A vulnerability in the GUI of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative privileges to upload files to an affected device. This vulnerability is due to improper validation of the file copy function. An attacker could exploit this vulnerability by sending a crafted file upload using the Cisco ISE GUI. A successful exploit could allow the attacker to upload arbitrary files to an affected system.	4.9	More Details
CVE-2025-9162	A flaw was found in org.keycloak/keycloak-model-storage-service. The KeycloakRealmImport custom resource substitutes placeholders within imported realm documents, potentially referencing environment variables. This substitution process allows for injection attacks when crafted realm documents are processed. An attacker can leverage this to inject malicious content during the realm import procedure. This can lead to unintended consequences within the Keycloak environment.	4.9	More Details
CVE-2025-8402	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.10.x <= 10.10.0, 10.9.x <= 10.9.3 fail to validate import data which allows a system admin to crash the server via the bulk import feature.	4.9	More Details
CVE-2025-20345	A vulnerability in the debug logging function of Cisco Duo Authentication Proxy could allow an authenticated, high-privileged, remote attacker to view sensitive information in a system log file. This vulnerability is due to insufficient masking of sensitive information before it is written to system log files. An attacker could exploit this vulnerability by accessing logs on an affected system. A successful exploit could allow the attacker to view sensitive information that should be restricted.	4.9	More Details

CVE-2025-49408	Insertion of Sensitive Information Into Sent Data vulnerability in WPDeveloper Templately allows Retrieve Embedded Sensitive Data. This issue affects Templately: from n/a through 3.2.7.	4.9	More Details
CVE-2025-54927	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause unauthorized access to sensitive files when an authenticated attackers uses a crafted path input that is processed by the system.	4.9	More Details
CVE-2025-55107	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.9.1 – 11.4 that may allow a remote, authenticated attacker to inject malicious a file with an embedded xss script which when loaded could potentially execute arbitrary JavaScript code in the victim’s browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2025-55104	A stored cross-site scripting (XSS) vulnerability exists ArcGIS HUB and ArcGIS Enterprise Sites which allows an authenticated user with the ability to create or edit a site to add and store an XSS payload. If this stored XSS payload is triggered by any user attacker supplied JavaScript may execute in the victim's browser.	4.8	More Details
CVE-2025-55105	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.9.1 – 11.4 that may allow a remote, authenticated attacker to inject malicious a file with an embedded xss script which when loaded could potentially execute arbitrary JavaScript code in the victim’s browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2025-55106	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.9.1 – 11.4 that may allow a remote, authenticated attacker to inject malicious a file with an embedded xss script which when loaded could potentially execute arbitrary JavaScript code in the victim’s browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2025-51990	XWiki through version 17.3.0 is affected by multiple stored Cross-Site Scripting (XSS) vulnerabilities in the Administration interface, specifically under the Presentation section of the Global Preferences panel. An authenticated administrator can inject arbitrary JavaScript payloads into the HTTP Meta Info, Footer Copyright, and Footer Version fields. These inputs are stored and subsequently rendered without proper output encoding or sanitization on public-facing pages. As a result, the injected scripts are persistently executed in the browser context of any visitor to the affected instances including both authenticated and unauthenticated users. No user interaction is required beyond visiting a page that includes the malicious content. Successful exploitation can lead to session hijacking, credential theft, unauthorized actions via session riding, or further compromise of the application through client-side attacks. The vulnerability introduces significant risk in any deployment, especially in shared or internet-facing environments where administrator credentials may be compromised.	4.8	More Details
CVE-2025-55103	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.9.1 – 11.4 that may allow a remote, authenticated attacker to inject malicious a file with an embedded xss script which when loaded could potentially execute arbitrary JavaScript code in the victim’s browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2025-9424	A vulnerability was identified in Ruijie WS7204-A 2017.06.15. Affected by this vulnerability is an unknown functionality of the file /itbox_pi/branch_import.php?a=branch_list. Such manipulation of the argument province leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-57727	In JetBrains IntelliJ IDEA before 2025.2 credentials disclosure was possible via remote reference	4.7	More Details
CVE-2025-6247	The WordPress Automatic Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.118.0. This is due to missing or incorrect nonce validation on one of its functions. This makes it possible for unauthenticated attackers to update campaigns 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.	4.7	More Details
CVE-2025-9414	A vulnerability was found in kalcaddle kodbox 1.61. Affected by this vulnerability is an unknown functionality of the file /?explorer/upload/serverDownload of the component Download from Link Handler. Performing manipulation of the argument url results in server-side request forgery. Remote exploitation of the attack is possible. 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.	4.7	More Details
CVE-2025-9296	A security vulnerability has been detected in Emlog Pro up to 2.5.18. This affects an unknown function of the file /admin/blogger.php?action=update_avatar. Such manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack 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.	4.7	More Details
CVE-2025-9402	A vulnerability was found in HuangDou UTCMS 9. This issue affects some unknown processing of the file app/modules/ut-frame/admin/update.php of the component Config Handler. Performing manipulation of the argument UPDATEURL results in server-side request forgery. The attack is possible to be carried out 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.	4.7	More Details
CVE-2025-9474	A vulnerability was detected in Mihomo Party up to 1.8.1 on macOS. Affected is the function enableSysProxy of the file src/main/sys/sysproxy.ts of the component Socket Handler. The manipulation results in creation of temporary file with insecure permissions. The attack requires a local approach. This attack is characterized by high complexity. The exploitability is told to be difficult. The exploit is now public and may be used.	4.5	More Details
CVE-2025-4877	There's a vulnerability in the libssh package where when a libssh consumer passes in an unexpectedly large input buffer to ssh_get_fingerprint_hash() function. In such cases the bin_to_base64() function can experience an integer overflow leading to a memory under allocation, when that happens it's possible that the program perform out of bounds write leading to a heap corruption. This issue affects only 32-bits builds of libssh.	4.5	More Details
CVE-2025-9431	A flaw has been found in mtons mblog up to 3.5.0. Impacted is an unknown function of the file /search. This manipulation of the argument kw causes cross site scripting. The attack can be initiated remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-	Missing Authorization vulnerability in themifyme Themify Builder allows Exploiting Incorrectly Configured Access Control Security Levels.	4.3	More

49396	This issue affects Themify Builder: from n/a through 7.6.7.		Details
CVE-2025-7839	The Restore Permanently delete Post or Page Data plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the rp_dpo_dpa_ajax_dp_delete_data() function. This makes it possible for unauthenticated attackers to delete data 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-2025-7221	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the give_update_payment_status() function in all versions up to, and including, 4.5.0. This makes it possible for authenticated attackers, with GiveWP Worker-level access and above, to update donations statuses. This ability is not present in the user interface.	4.3	More Details
CVE-2025-7828	The WP Filter & Combine RSS Feeds plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the post_listing_page() function in all versions up to, and including, 0.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete feeds.	4.3	More Details
CVE-2025-9202	The ColorMag theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the welcome_notice_import_handler() function in all versions up to, and including, 4.0.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install the ThemeGrill Demo Importer plugin.	4.3	More Details
CVE-2025-7827	The Ni WooCommerce Customer Product Report plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ni_woocpr_action() function in all versions up to, and including, 1.2.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update plugin settings.	4.3	More Details
CVE-2025-49391	Cross-Site Request Forgery (CSRF) vulnerability in Fetch Designs Sign-up Sheets allows Cross Site Request Forgery. This issue affects Sign-up Sheets: from n/a through 2.3.3.	4.3	More Details
CVE-2025-9263	A vulnerability has been found in Xuxueli xxl-job up to 3.1.1. Affected by this vulnerability is the function getJobsByGroup of the file /src/main/java/com/xxl/job/admin/controller/JobLogController.java. Such manipulation of the argument jobGroup leads to improper control of resource identifiers. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7841	The Sertifier Certificate & Badge Maker for WordPress – Tutor LMS plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.19. This is due to missing or incorrect nonce validation on the 'sertifier_settings' page. This makes it possible for unauthenticated attackers to update the plugin's api key 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-2025-9240	A security flaw has been discovered in elunez eladmin up to 2.7. Affected by this issue is some unknown functionality of the file /auth/info. The manipulation results in information disclosure. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-9331	The Spacious theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'welcome_notice_import_handler' function in all versions up to, and including, 1.9.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import demo data into the site.	4.3	More Details
CVE-2025-9432	A vulnerability has been found in mtons mblog up to 3.5.0. The affected element is an unknown function of the file /admin/post/list of the component Admin Panel. Such manipulation of the argument Title leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-9433	A vulnerability was found in mtons mblog up to 3.5.0. The impacted element is an unknown function of the file /admin/user/list of the component Admin Panel. Performing manipulation of the argument Name results in cross site scripting. The attack may be initiated remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2024-8860	The Tourfic plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the tf_order_status_email_resend_function, tf_visitor_details_edit_function, tf_checkinout_details_edit_function, tf_order_status_edit_function, tf_order_bulk_action_edit_function, tf_remove_room_order_ids, and tf_delete_old_review_fields functions in all versions up to, and including, 2.14.5. This makes it possible for authenticated attackers, with subscriber-level access and above, to resend order status emails, update visitor/order details, edit check-in/out details, edit order status, perform bulk order status updates, remove room order IDs, and delete old review fields, respectively.	4.3	More Details
CVE-2025-55744	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. Before 0.2.1, some of the endpoints of the application is vulnerable to Cross site Request forgery (CSRF). This vulnerability is fixed in 0.2.1.	4.3	More Details
CVE-2025-57895	Cross-Site Request Forgery (CSRF) vulnerability in Hossni Mubarak JobWP allows Cross Site Request Forgery. This issue affects JobWP: from n/a through 2.4.3.	4.3	More Details
CVE-2025-57894	Missing Authorization vulnerability in ollybach WPPizza allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WPPizza: from n/a through 3.19.8.	4.3	More Details
CVE-2025-57893	Cross-Site Request Forgery (CSRF) vulnerability in Epsiloncool WP Fast Total Search allows Cross Site Request Forgery. This issue affects WP Fast Total Search: from n/a through 1.79.270.	4.3	More Details
CVE-2025-57892	Cross-Site Request Forgery (CSRF) vulnerability in Jeff Starr Simple Statistics for Feeds allows Cross Site Request Forgery. This issue affects Simple Statistics for Feeds: from n/a through 20250322.	4.3	More Details
CVE-2025-9440	A security vulnerability has been detected in 1000projects Online Project Report Submission and Evaluation System 1.0. Affected by this issue is some unknown functionality of the file /admin/add_title.php. Such manipulation of the argument Title leads to cross site scripting. The attack may be performed from a remote location. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-7842	The Silencesoft RSS Reader plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.6. This is due to missing or incorrect nonce validation on the 'sil_rss_edit_page' page. This makes it possible for unauthenticated attackers to delete RSS feeds 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-2025-9439	A weakness has been identified in 1000projects Online Project Report Submission and Evaluation System 1.0. Affected by this vulnerability is an unknown functionality of the file /rse/admin/edit_faculty.php?id=2. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-57885	Cross-Site Request Forgery (CSRF) vulnerability in Shahjahan Jewel Fluent Support allows Cross Site Request Forgery. This issue affects Fluent Support: from n/a through 1.9.1.	4.3	More Details
CVE-2025-9438	A security flaw has been discovered in 1000projects Online Project Report Submission and Evaluation System 1.0. Affected is an unknown function of the file /admin/add_student.php. The manipulation of the argument address results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-57884	Missing Authorization vulnerability in wpsoul Greenshift allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Greenshift: from n/a through 12.1.1.	4.3	More Details
CVE-2025-47870	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.9.x <= 10.9.2 fail to sanitize the team invite ID in the POST /api/v4/teams/:teamId/restore endpoint which allows an team admin with no member invite privileges to get the team’s invite id.	4.3	More Details
CVE-2025-49426	Cross-Site Request Forgery (CSRF) vulnerability in Dourou Cookie Warning allows Cross Site Request Forgery. This issue affects Cookie Warning: from n/a through 1.3.	4.3	More Details
CVE-2025-9434	A vulnerability was determined in 1000projects Online Project Report Submission and Evaluation System 1.0. This affects an unknown function of the file /admin/edit_title.php?id=1. Executing manipulation of the argument desc can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2025-1501	An access control vulnerability was discovered in the Request Trace and Download Trace functionalities of CMC before 25.1.0 due to a specific access restriction not being properly enforced for users with limited privileges. An authenticated user with limited privileges can request and download trace files due to improper access restrictions, potentially exposing unauthorized network data.	4.3	More Details
CVE-2025-9461	A weakness has been identified in diyhi bbs up to 6.8. The impacted element is an unknown function of the file src/main/java/cms/web/action/filePackage/FilePackageManageAction.java of the component File Compression Handler. This manipulation of the argument idGroup causes information disclosure. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	4.3	More Details
CVE-2025-49896	Cross-Site Request Forgery (CSRF) vulnerability in wptasker WP Discord Post Plus – Supports Unlimited Channels allows Cross Site Request Forgery. This issue affects WP Discord Post Plus – Supports Unlimited Channels: from n/a through 1.0.2.	4.3	More Details
CVE-2025-54551	Synapse Mobility 8.0, 8.0.1, 8.0.2, 8.1, and 8.1.1 contain a privilege escalation vulnerability through external control of Web parameter. If exploited, a user of the product may escalate the privilege and access data that the user do not have permission to view by altering the parameters of the search function.	4.3	More Details
CVE-2025-9409	A security flaw has been discovered in lostvip-com ruoyi-go up to 2.1. Impacted is the function DownloadTmp/DownloadUpload of the file modules/system/controller/CommonController.go. Performing manipulation of the argument fileName results in path traversal. 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-2025-48303	Cross-Site Request Forgery (CSRF) vulnerability in Kevin Langley Jr. Post Type Converter allows Cross-Site Request Forgery.This issue affects Post Type Converter: from n/a through 0.6.	4.3	More Details
CVE-2025-6465	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 10.10.x <= 10.10.0, 10.9.x <= 10.9.3 fail to sanitize file names which allows users with file upload permission to overwrite file attachment thumbnails via path traversal in file streaming APIs.	4.3	More Details
CVE-2025-9228	MiR software versions prior to version 3.0.0 have insufficient authorization controls when creating text notes, allowing low-privilege users to create notes which are intended only for administrative users.	4.3	More Details
CVE-2025-57734	In JetBrains TeamCity before 2025.07.1 aWS credentials were exposed in Docker script files	4.3	More Details
CVE-2025-35112	Agiloft Release 28 contains an XML External Entities vulnerability in any table that allows 'import/export', allowing an authenticated attacker to import the template file and perform path traversal on the local system files. Users should upgrade to Agiloft Release 31.	4.1	More Details
CVE-2025-53971	Mattermost versions 10.5.x <= 10.5.8, 9.11.x <= 9.11.17 fail to properly validate authorization for team scheme role modifications which allows Team Admins to demote Team Members to Guests via the PUT /api/v4/teams/team-id/members/user-id/schemeRoles API endpoint.	3.8	More Details
CVE-2025-3456	On affected platforms running Arista EOS, the global common encryption key configuration may be logged in clear text, in local or remote accounting logs. Knowledge of both the encryption key and protocol specific encrypted secrets from the device running-config could then be used to obtain protocol specific passwords in cases where symmetric passwords are required between devices with neighbor protocol relationships.	3.8	More Details
CVE-2025-55212	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-28 and 7.1.2-2, passing a geometry string containing only a colon (":") to montage -geometry leads GetGeometry() to set width/height to 0. Later, ThumbnailImage() divides by these zero dimensions, triggering a crash (SIGFPE/abort), resulting in a denial of service. This issue has been patched in versions 6.9.13-28 and 7.1.2-2.	3.7	More Details
CVE-	A vulnerability has been found in HuangDou UTCMS 9. This vulnerability affects unknown code of the file app/modules/ut-		

2025-9401	frame/admin/login.php of the component Login. Such manipulation of the argument code leads to incorrect comparison. The attack can be executed remotely. The attack requires a high level of complexity. It is stated that the exploitability is difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-9239	A vulnerability was identified in elunez eladmin up to 2.7. Affected by this vulnerability is the function EncryptUtils of the file eladmin-common/src/main/java/me/zhengjie/utils/EncryptUtils.java of the component DES Key Handler. The manipulation of the argument STR_PARAM with the input Passw0rd leads to inadequate encryption strength. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitation appears to be difficult.	3.7	More Details
CVE-2025-9429	A security vulnerability has been detected in mtons mblog up to 3.5.0. This vulnerability affects unknown code of the file /post/submit of the component Post Handler. The manipulation of the argument content/title/ leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2025-9233	A security vulnerability has been detected in Scada-LTS up to 2.7.8.1. Impacted is an unknown function of the file view_edit.shtm. The manipulation of the argument Name leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2025-55455	DooTask v1.0.51 was dicovered to contain an authenticated arbitrary download vulnerability via the component /msg/sendtext.	3.5	More Details
CVE-2025-9407	A flaw has been found in mtons mblog up to 3.5.0. Affected by this vulnerability is an unknown functionality of the file /settings/profile. Executing manipulation of the argument signature can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2025-49810	Mattermost versions 10.5.x <= 10.5.8 fail to validate access controls at time of access which allows user to read a thread via AI posts	3.5	More Details
CVE-2025-9234	A vulnerability was detected in Scada-LTS up to 2.7.8.1. The affected element is an unknown function of the file maintenance_events.shtm. The manipulation of the argument Alias results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2025-9235	A flaw has been found in Scada-LTS up to 2.7.8.1. The impacted element is an unknown function of the file compound_events.shtm. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used.	3.5	More Details
CVE-2025-9193	A flaw has been found in TOTVS Portal Meu RH up to 12.1.17. Impacted is an unknown function of the component Password Reset Handler. Executing manipulation of the argument redirectUrl can lead to open redirect. The attack may be performed from a remote location. The exploit has been published and may be used. Upgrading to version 12.1.2410.274, 12.1.2502.178 and 12.1.2506.121 is recommended to address this issue. It is recommended to upgrade the affected component. The vendor explains, that "[o]ur internal validation (...) confirms that the reported behavior does not exist in currently supported releases. In these tests, the redirectUrl parameter is ignored, and no malicious redirection occurs." This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2025-47700	Mattermost Server versions 10.5.x <= 10.5.9 utilizing the Agents plugin fail to reject empty request bodies which allows users to trick users into clicking malicious links via post actions	3.5	More Details
CVE-2025-9388	A vulnerability was determined in Scada-LTS up to 2.7.8.1. This impacts an unknown function of the file watch_list.shtm. 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-2025-9237	A vulnerability was found in CodeAstro Ecommerce Website 1.0. This impacts an unknown function of the file /customer/my_account.php?edit_account of the component Edit Your Account Page. Performing manipulation of the argument Username results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	3.5	More Details
CVE-2025-9306	A vulnerability was detected in SourceCodester Advanced School Management System 1.0. The impacted element is an unknown function of the file /index.php/notice/addNotice. The manipulation of the argument noticeSubject results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2025-55523	An issue in the component /api/download_work_dir_file.py of Agent-Zero v0.8.* allows attackers to execute a directory traversal.	3.5	More Details
CVE-2025-9403	A vulnerability was determined in jqlang jq up to 1.6. Impacted is the function run_jq_tests of the file jq_test.c of the component JSON Parser. Executing manipulation can lead to reachable assertion. The attack requires local access. The exploit has been publicly disclosed and may be utilized. Other versions might be affected as well.	3.3	More Details
CVE-2025-9396	A security flaw has been discovered in ckolivas lrzip up to 0.651. This impacts the function __GI____strtol_l_internal of the file strtol_l.c. Performing manipulation results in null pointer dereference. The attack is only possible with local access. The exploit has been released to the public and may be exploited.	3.3	More Details
CVE-2025-9301	A vulnerability was determined in cmake 4.1.20250725-gb5cce23. This affects the function cmForEachFunctionBlocker::ReplayItems of the file cmForEachCommand.cxx. This manipulation causes reachable assertion. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. Patch name: 37e27f71bc356d880c908040cd0cb68fa2c371b8. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2025-9384	A vulnerability was detected in appneta tcpreplay up to 4.5.1. Impacted is the function tcpedit_post_args of the file /src/tcpedit/parse_args.c. The manipulation results in null pointer dereference. The attack is only possible with local access. The exploit is now public and may be used. Upgrading to version 4.5.2-beta2 is recommended to address this issue. Upgrading the affected component is advised. The vendor explains, that he was "[a]ble to reproduce in 6fcbf03 but not in 4.5.2-beta2".	3.3	More Details
CVE-2025-9308	A vulnerability has been found in yarnpkg Yarn up to 1.22.22. This impacts the function setOptions of the file src/util/request-manager.js. Such manipulation leads to inefficient regular expression complexity. Local access is required to approach this attack. This vulnerability only affects products that are no longer supported by the maintainer.	3.3	More Details
CVE-	A vulnerability was identified in vim 9.1.0000. Affected is the function __memmove_avx_unaligned_erms of the file memmove-vec-unaligned-erms.S. The manipulation leads to memory corruption. The attack needs to be performed locally. The exploit is publicly		More

2025-9389	available and might be used. Some users are not able to reproduce this. One of the users mentions that this appears not to be working, "when coloring is turned on".	3.3	Details
CVE-2025-9383	A security vulnerability has been detected in FNKvision Y215 CCTV Camera 10.194.120.40. This issue affects the function crypt of the file /etc/passwd. The manipulation leads to use of weak hash. The attack can only be performed from a local environment. The complexity of an attack is rather high. The exploitability is assessed as difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.5	More Details
CVE-2025-9309	A vulnerability was found in Tenda AC10 16.03.10.13. Affected is an unknown function of the file /etc_ro/shadow of the component MD5 Hash Handler. Performing manipulation results in hard-coded credentials. The attack needs to be approached locally. A high degree of complexity is needed for the attack. The exploitability is told to be difficult. The exploit has been made public and could be used.	2.5	More Details
CVE-2025-9416	A security flaw has been discovered in oitcode samarium up to 0.9.6. This vulnerability affects unknown code of the file /cms/webpage/ of the component Pages Image Handler. The manipulation results in cross site scripting. The attack may be performed from a remote location. The exploit has been released to the public and may be exploited.	2.4	More Details
CVE-2025-9430	A vulnerability was detected in mtons mblog up to 3.5.0. This issue affects some unknown processing of the file /admin/options/update. The manipulation of the argument input results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2025-9422	A vulnerability was found in oitcode samarium up to 0.9.6. This impacts an unknown function of the file /dashboard/team of the component Team Image Handler. The manipulation results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used.	2.4	More Details
CVE-2025-9404	A vulnerability was identified in Scada-LTS up to 2.7.8.1. The affected element is an unknown function of the file /pointHierarchySLTS of the component Folder Handler. The manipulation of the argument Title leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2.4	More Details
CVE-2025-8448	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could cause unauthorized access to sensitive credential data when an attacker is able to capture local SMB traffic between a valid user within the BMS network and the vulnerable products.	2.3	More Details
CVE-2025-9381	A security flaw has been discovered in FNKvision Y215 CCTV Camera 10.194.120.40. This affects an unknown part of the file /tmp/wpa_supplicant.conf. Performing manipulation results in information disclosure. The attack may be carried out on the physical device. The attack's complexity is rated as high. It is indicated that the exploitability is difficult. 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.	1.6	More Details
CVE-2010-20107	A stack-based buffer overflow exists in FTP Synchronizer Professional <= v4.0.73.274. When the client connects to an FTP server and issues a LIST command—typically during sync preview or profile creation—the server’s response containing an overly long filename triggers a buffer overflow. This results in the corruption of the Structured Exception Handler (SEH), potentially allowing remote code execution.	N/A	More Details
CVE-2025-57814	request-filtering-agent is an http(s).Agent implementation that blocks requests to Private/Reserved IP addresses. Versions 1.x.x and earlier contain a vulnerability where HTTPS requests to 127.0.0.1 bypass IP address filtering, while HTTP requests are correctly blocked. This allows attackers to potentially access internal HTTPS services running on localhost, bypassing the library's SSRF protection. The vulnerability is particularly dangerous when the application accepts user-controlled URLs and internal services are only protected by network-level restrictions. This vulnerability has been fixed in request-filtering-agent version 2.0.0. Users should upgrade to version 2.0.0 or later.	N/A	More Details
CVE-2010-20034	Gekko Manager FTP Client <= 0.77 contains a stack-based buffer overflow in its FTP directory listing parser. When processing a server response to a LIST command, the client fails to properly validate the length of filenames. A crafted response containing an overly long filename can overwrite the Structured Exception Handler (SEH), potentially allowing remote code execution.	N/A	More Details
CVE-2025-43750	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.1, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 and 7.4 GA through update 92 allows remote unauthenticated users (guests) to upload files via the form attachment field without proper validation, enabling extension obfuscation and bypassing MIME type checks.	N/A	More Details
CVE-2025-3478	A Stored Cross-Site Scripting (XSS) vulnerability has been identified in OpenText Enterprise Security Manager. The vulnerability could be remotely exploited.	N/A	More Details
CVE-2025-57805	The Scratch Channel is a news website. In versions 1 and 1.1, a POST request to the endpoint used to publish articles, can be used to post an article in any category with any date, regardless of who's logged in. This issue has been patched in version 1.2.	N/A	More Details
CVE-2010-20007	Seagull FTP Client <= v3.3 Build 409 contains a stack-based buffer overflow vulnerability in its FTP directory listing parser. When the client connects to an FTP server and receives a crafted response to a LIST command containing an excessively long filename, the application fails to properly validate input length, resulting in a buffer overflow that overwrites the Structured Exception Handler (SEH). This may allow remote attackers to execute arbitrary code on the client system. This product line was discontinued and users were advised to use BlueZone Secure FTP instead, at the time of disclosure.	N/A	More Details
CVE-2025-54172	QuickCMS is vulnerable to Stored XSS in sTitle parameter in page editor functionality. Malicious attacker with admin privileges can inject arbitrary HTML and JS into website, which will be rendered/executed when visiting edited page. Regular admin user is not able to inject any JS scripts into the page. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-57809	XGrammar is an open-source library for efficient, flexible, and portable structured generation. Prior to version 0.1.21, XGrammar has an infinite recursion issue in the grammar. This issue has been resolved in version 0.1.21.	N/A	More Details
CVE-2025-8447	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed users with access to any repository to retrieve limited code content from another repository by creating a diff between the repositories. To exploit this vulnerability, an attacker needed to know the name of a private repository along with its branches, tags, or commit SHAs that they could use to trigger compare/diff functionality and retrieve limited code without proper authorization. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.18, and was fixed in versions 3.14.17, 3.15.12, 3.16.8 and 3.17.5. This vulnerability was reported via the	N/A	More Details

	GitHub Bug Bounty program.		
CVE-2025-43749	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.1, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows unauthenticated users (guests) to access via URL files uploaded in the form and stored in document_library	N/A	More Details
CVE-2025-57772	DataEase is an open source business intelligence and data visualization tool. Prior to version 2.10.12, there is a H2 JDBC RCE bypass in DataEase. If the JDBC URL meets criteria, the getJdbcUrl method is returned, which acts as the getter for the JdbcUrl parameter provided. This bypasses H2's filtering logic and returns the H2 JDBC URL, allowing the "driver":"org.h2.Driver" to specify the H2 driver for the JDBC connection. The vulnerability has been fixed in version 2.10.12.	N/A	More Details
CVE-2025-43742	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.3, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript in web content for friendly urls.	N/A	More Details
CVE-2025-57773	DataEase is an open source business intelligence and data visualization tool. Prior to version 2.10.12, because DB2 parameters are not filtered, a JNDI injection attack can be directly launched. JNDI triggers an AspectJWeaver deserialization attack, writing to various files. This vulnerability requires commons-collections 4.x and aspectjweaver-1.9.22.jar. The vulnerability has been fixed in version 2.10.12.	N/A	More Details
CVE-2025-43741	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.3, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows an remote authenticated attacker to inject JavaScrip in the _com_liferay_users_admin_web_portlet_UsersAdminPortlet_assetTagNames parameter	N/A	More Details
CVE-2009-20004	gAlan 0.2.1, a modular audio processing environment for Windows, is vulnerable to a stack-based buffer overflow when parsing .galan files. The application fails to properly validate the length of input data, allowing a specially crafted file to overwrite the stack and execute arbitrary code. Exploitation requires local interaction, typically by convincing a user to open the malicious file.	N/A	More Details
CVE-2009-20003	Xenorate versions up to and including 2.50, a Windows-based multimedia player, is vulnerable to a stack-based buffer overflow when processing .xpl playlist files. The application fails to properly validate the length of input data, allowing an attacker to craft a malicious .xpl file that overwrites the Structured Exception Handler (SEH) and enables arbitrary code execution. Exploitation requires local interaction, typically by convincing a user to open the crafted file.	N/A	More Details
CVE-2025-50383	alextselegidis Easy!Appointments v1.5.1 was discovered to contain a SQL injection vulnerability via the order_by parameter.	N/A	More Details
CVE-2025-57811	Craft is a platform for creating digital experiences. From versions 4.0.0-RC1 to 4.16.5 and 5.0.0-RC1 to 5.8.6, there is a potential remote code execution vulnerability via Twig SSTI (Server-Side Template Injection). This is a follow-up to CVE-2024-52293. This vulnerability has been patched in versions 4.16.6 and 5.8.7.	N/A	More Details
CVE-2009-20002	Millenium MP3 Studio versions up to and including 2.0 is vulnerable to a stack-based buffer overflow when parsing .pls playlist files. The application fails to properly validate the length of the File1 field within the playlist, allowing an attacker to craft a malicious .pls file that overwrites the Structured Exception Handler (SEH) and executes arbitrary code. Exploitation requires the victim to open the file locally, though remote execution may be possible if the .pls extension is registered to the application and opened via a browser.	N/A	More Details
CVE-2025-8627	The TP-Link KP303 Smartplug can be issued unauthenticated protocol commands that may cause unintended power-off condition and potential information leak. This issue affects TP-Link KP303 (US) Smartplug: before 1.1.0.	N/A	More Details
CVE-2025-34158	Plex Media Server (PMS) versions 1.41.7.x through 1.42.0.x are affected by an unspecified security vulnerability reported via Plex’s bug bounty program. While technical details have not been publicly disclosed, the issue was acknowledged by the vendor and resolved in version 1.42.1. The vulnerability may pose a risk to system integrity, confidentiality, or availability, prompting a strong recommendation for all users to upgrade immediately.	N/A	More Details
CVE-2025-57804	h2 is a pure-Python implementation of a HTTP/2 protocol stack. Prior to version 4.3.0, an HTTP/2 request splitting vulnerability allows attackers to perform request smuggling attacks by injecting CRLF characters into headers. This occurs when servers downgrade HTTP/2 requests to HTTP/1.1 without properly validating header names/values, enabling attackers to manipulate request boundaries and bypass security controls. This issue has been patched in version 4.3.0.	N/A	More Details
CVE-2025-57802	Airlink's Daemon interfaces with Docker and the Panel to provide secure access for controlling instances via the Panel. In version 1.0.0, an attacker with access to the affected container can create symbolic links inside the mounted directory (/app/data). Because the container bind-mounts an arbitrary host path, these symlinks can point to sensitive locations on the host filesystem. When the application or other processes follow these symlinks, the attacker can gain unauthorized read access to host files outside the container. This issue has been patched in version 1.0.1.	N/A	More Details
CVE-2025-38623	In the Linux kernel, the following vulnerability has been resolved: PCI: pnv_php: Fix surprise plug detection and recovery The existing PowerNV hotplug code did not handle surprise plug events correctly, leading to a complete failure of the hotplug system after device removal and a required reboot to detect new devices. This comes down to two issues: 1) When a device is surprise removed, often the bridge upstream port will cause a PE freeze on the PHB. If this freeze is not cleared, the MSI interrupts from the bridge hotplug notification logic will not be received by the kernel, stalling all plug events on all slots associated with the PE. 2) When a device is removed from a slot, regardless of surprise or programmatic removal, the associated PHB/PE ls left frozen. If this freeze is not cleared via a fundamental reset, skiboot is unable to clear the freeze and cannot retrain / rescan the slot. This also requires a reboot to clear the freeze and redetect the device in the slot. Issue the appropriate unfreeze and rescan commands on hotplug events, and don't oops on hotplug if pci_bus_to_OF_node() returns NULL. [bhelgaas: tidy comments]	N/A	More Details
CVE-2025-55297	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. The BluFi example bundled in ESP-IDF was vulnerable to memory overflows in two areas: Wi-Fi credential handling and Diffie–Hellman key exchange. This vulnerability is fixed in 5.4.1, 5.3.3, 5.1.6, and 5.0.9.	N/A	More Details
CVE-2025-57746	Rejected reason: Not used	N/A	More Details
CVE-2025-0081	In dng_lossless_decoder::HuffDecode of dng_lossless_jpeg.cpp, there is a possible way to cause a crash due to uninitialized data. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details

CVE-2025-0080	In multiple locations, there is a possible way to overlay the installation confirmation dialog due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-0079	In multiple locations, there is a possible way that avdtp and avctp channels could be unencrypted due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-0078	In main of main.cpp, there is a possible way to bypass SELinux due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-0075	In process_service_search_attr_req of sdp_server.cc, there is a possible way to execute arbitrary code 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.	N/A	More Details
CVE-2025-0074	In process_service_attr_rsp of sdp_discovery.cc, there is a possible way to execute arbitrary code 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.	N/A	More Details
CVE-2024-49740	In multiple locations, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2023-21125	In btif_hh_hsdata_rpt_copy_cb of bta_hh.cc, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-54364	Microsoft Knack 0.12.0 allows Regular expression Denial of Service (ReDoS) in the knack.introspection module. option_descriptions employs an inefficient regular expression pattern: "\s(:param)\s+(.+?)\s:(.*)" that is susceptible to catastrophic backtracking when processing crafted docstrings containing a large volume of whitespace without a terminating colon. An attacker who can control or inject docstring content into affected applications can trigger excessive CPU consumption. This software is used by Azure CLI.	N/A	More Details
CVE-2024-47192	An issue was discovered in Mahara 23.04.8 and 24.04.4. The use of a malicious export download URL can allow an attacker to download files that they do not have permission to download.	N/A	More Details
CVE-2024-35203	Mahara before 22.10.6, 23.04.6, and 24.04.1 allows cross-site scripting (XSS) via a file, with JavaScript code as part of its name, that is uploaded via the Mahara filebrowser system.	N/A	More Details
CVE-2025-55443	Telpo MDM 1.4.6 thru 1.4.9 for Android contains sensitive administrator credentials and MQTT server connection details (IP/port) that are stored in plaintext within log files on the device's external storage. This allows attackers with access to these logs to: 1. Authenticate to the MDM web platform to execute administrative operations (device shutdown/factory reset/software installation); 2. Connect to the MQTT server to intercept/publish device data.	N/A	More Details
CVE-2025-52353	An arbitrary code execution vulnerability in Badaso CMS 2.9.11. The Media Manager allows authenticated users to upload files containing embedded PHP code via the file-upload endpoint, bypassing content-type validation. When such a file is accessed via its URL, the server executes the PHP payload, enabling an attacker to run arbitrary system commands and achieve full compromise of the underlying host. This has been demonstrated by embedding a backdoor within a PDF and renaming it with a .php extension.	N/A	More Details
CVE-2025-50971	Directory traversal vulnerability in AbanteCart version 1.4.2 allows unauthenticated attackers to gain access to sensitive system files via the template parameter to index.php.	N/A	More Details
CVE-2025-9478	Use after free in ANGLE in Google Chrome prior to 139.0.7258.154 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	N/A	More Details
CVE-2025-50975	IPFire 2.29 web-based firewall interface (firewall.cgi) fails to sanitize several rule parameters such as PROT, SRC_PORT, TGT_PORT, dnatport, key, ruleremark, src_addr, std_net_tgt, and tgt_addr, allowing an authenticated administrator to inject persistent JavaScript. This stored XSS payload is executed whenever another admin views the firewall rules page, enabling session hijacking, unauthorized actions within the interface, or further internal pivoting. Exploitation requires only high-privilege GUI access, and the complexity of the attack is low.	N/A	More Details
CVE-2025-57742	Rejected reason: Not used	N/A	More Details
CVE-2025-57743	Rejected reason: Not used	N/A	More Details
CVE-2025-57744	Rejected reason: Not used	N/A	More Details
CVE-2025-0082	In multiple functions of StatusHint.java and TelecomServiceImpl.java, there is a possible way to reveal images across users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	N/A	More Details
CVE-2025-0083	In multiple locations, there is a possible way to access content across user profiles due to URI double encoding. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-	In multiple locations, there is a possible out of bounds write due to a use after free. This could lead to remote code execution over Bluetooth, if HFP support is enabled, with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details

0084			
CVE-2025-22410	In multiple locations, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-57820	Svelte devalue is a utility library. Prior to version 5.3.2, a string passed to devalue.parse could represent an object with a __proto__ property and devalue.parse does not check that an index is numeric. This could result in assigning prototypes to objects and properties, leading to prototype pollution. This issue has been fixed in version 5.3.2	N/A	More Details
CVE-2024-12223	Prism Central versions prior to 2024.3.1 are vulnerable to a stored cross-site scripting attack via the Events component, allowing an attacker to hijack a victim user’s session and perform actions in their security context.	N/A	More Details
CVE-2025-54363	Microsoft Knack 0.12.0 allows Regular expression Denial of Service (ReDoS) in the knack.introspection module. extract_full_summary_from_signature employs an inefficient regular expression pattern: "\s(:param)\s+(.+?)\s:(.*)" that is susceptible to catastrophic backtracking when processing crafted docstrings containing a large volume of whitespace without a terminating colon. An attacker who can control or inject docstring content into affected applications can trigger excessive CPU consumption. This software is used by Azure CLI.	N/A	More Details
CVE-2025-43756	<!--td {border: 1px solid #cccccc;}br {mso-data-placement:same-cell;}-->A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.15, 2025.Q2.0 through 2025.Q2.2 and 2024.Q1.13 through 2024.Q1.19 allows a remote authenticated user to inject JavaScript code via snippet parameter.	N/A	More Details
CVE-2025-26417	In checkWhetherCallingAppHasAccess of DownloadProvider.java, there is a possible bypass of user consent when opening files in shared storage due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22413	In multiple functions of hyp-main.c, there is a possible privilege escalation due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22412	In multiple functions of sdp_server.cc, there is a possible use after free due to a logic error in the code. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22411	In process_service_attr_rsp of sdp_discovery.cc, there is a possible use after free due to a logic error in the code. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22409	In rfc_send_buf_uih of rfc_ts_frames.cc, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-0086	In onResult of AccountManagerService.java, there is a possible way to overwrite auth token due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22408	In rfc_check_send_cmd of rfc_utils.cc, there is a possible way to execute arbitrary code 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.	N/A	More Details
CVE-2025-22407	In hidd_check_config_done of hidd_conn.cc, there is a possible way to execute arbitrary code due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22406	In bnepu_check_send_packet of bnep_utils.cc, there is a possible way to achieve code execution due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22405	In multiple locations, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22404	In avct_lcb_msg_ind of avct_lcb_act.cc, there is a possible way to execute arbitrary code due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2025-22403	In sdp_snd_service_search_req of sdp_discovery.cc, there is a possible way to execute arbitrary code 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.	N/A	More Details
CVE-2025-0093	In handleBondStateChanged of AdapterService.java, there is a possible unapproved data access due to a missing permission check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	N/A	More Details
CVE-2025-0092	In handleBondStateChanged of AdapterService.java, there is a possible permission bypass due to misleading or insufficient UI. This could lead to remote (proximal/adjacent) information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	N/A	More Details
CVE-2025-57745	Rejected reason: Not used	N/A	More Details
CVE-2025-43755	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 t through 7.4.3.132, and Liferay DXP 2025.Q2.0, 2025.Q1.0 through 2025.Q1.13, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.17 and 7.4 GA through update 92 allows an remote authenticated attacker to inject JavaScript into the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_type parameter.	N/A	More Details

CVE-2010-20121	EasyFTP Server versions up to 1.7.0.11 contain a stack-based buffer overflow vulnerability in the FTP command parser. When processing the CWD (Change Working Directory) command, the server fails to properly validate the length of the input string, allowing attackers to overwrite memory on the stack. This flaw enables remote code execution without authentication, as EasyFTP allows anonymous access by default. The vulnerability was resolved in version 1.7.0.12, after which the product was renamed “UplusFtp.”	N/A	More Details
CVE-2025-57747	Rejected reason: Not used	N/A	More Details
CVE-2024-47853	An issue was discovered in Mahara 23.04.8 and 24.04.4. Attackers may utilize escalation of privileges in certain cases when logging into Mahara with Learning Tools Interoperability (LTI).	N/A	More Details
CVE-2025-57753	vite-plugin-static-copy is rollup-plugin-copy for Vite with dev server support. Files not included in src are accessible with a crafted request. The vulnerability is fixed in 2.3.2 and 3.1.2.	N/A	More Details
CVE-2025-9190	The configuration of Cursor on macOS, specifically the "RunAsNode" fuse enabled, allows a local attacker with unprivileged access to execute arbitrary code that inherits Cursor TCC (Transparency, Consent, and Control) permissions. Acquired resource access is limited to previously granted permissions by the user. Accessing other resources beyond previously granted TCC permissions will prompt the user for approval in the name of Cursor, potentially disguising attacker's malicious intent. This issue was detected in 15.4.1 version of Cursor. Project maintainers decided not to fix this issue, because a scenario including a local attacker falls outside their defined threat model.	N/A	More Details
CVE-2025-8700	Invoice Ninja's configuration on macOS, specifically the presence of entitlement "com.apple.security.get-task-allow", allows local attackers with unprivileged access (e.g. via a malicious application) to attach a debugger, read or modify the process memory, inject code in the application's context despite being signed with Hardened Runtime and bypass Transparency, Consent, and Control (TCC). Acquired resource access is limited to previously granted permissions by the user. Access to other resources beyond granted permissions requires user interaction with a system prompt asking for permission. According to Apple documentation, when a non-root user runs an app with the debugging tool entitlement, the system presents an authorization dialog asking for a system administrator's credentials. Since there is no prompt when the target process has "get-task-allow" entitlement, the presence of this entitlement was decided to be treated as a vulnerability because it removes one step needed to perform an attack. This issue was fixed in version 5.0.175	N/A	More Details
CVE-2025-8597	MacVim's configuration on macOS, specifically the presence of entitlement "com.apple.security.get-task-allow", allows local attackers with unprivileged access (e.g. via a malicious application) to attach a debugger, read or modify the process memory, inject code in the application's context despite being signed with Hardened Runtime and bypass Transparency, Consent, and Control (TCC). Acquired resource access is limited to previously granted permissions by the user. Access to other resources beyond granted permissions requires user interaction with a system prompt asking for permission. According to Apple documentation, when a non-root user runs an app with the debugging tool entitlement, the system presents an authorization dialog asking for a system administrator's credentials. Since there is no prompt when the target process has "get-task-allow" entitlement, the presence of this entitlement was decided to be treated as a vulnerability because it removes one step needed to perform an attack. This issue was fixed in build r181.2	N/A	More Details
CVE-2025-7776	Memory overflow vulnerability leading to unpredictable or erroneous behavior and Denial of Service in NetScaler ADC and NetScaler Gateway when NetScaler is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) with PCoIP Profile bounded to it	N/A	More Details
CVE-2025-7775	Memory overflow vulnerability leading to Remote Code Execution and/or Denial of Service in NetScaler ADC and NetScaler Gateway when NetScaler is configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server (OR) NetScaler ADC and NetScaler Gateway 13.1, 14.1, 13.1-FIPS and NDcPP: LB virtual servers of type (HTTP, SSL or HTTP_QUIC) bound with IPv6 services or servicegroups bound with IPv6 servers (OR) NetScaler ADC and NetScaler Gateway 13.1, 14.1, 13.1-FIPS and NDcPP: LB virtual servers of type (HTTP, SSL or HTTP_QUIC) bound with DBS IPv6 services or servicegroups bound with IPv6 DBS servers (OR) CR virtual server with type HDX	N/A	More Details
CVE-2025-53813	The configuration of Nozbe on macOS, specifically the "RunAsNode" fuse enabled, allows a local attacker with unprivileged access to execute arbitrary code that inherits Nozbe TCC (Transparency, Consent, and Control) permissions. Acquired resource access is limited to previously granted permissions by the user. Access to other resources beyond granted-permissions requires user interaction with a system prompt asking for permission. This issue was fixed in version 2025.11 of Nozbe.	N/A	More Details
CVE-2025-53811	The configuration of Mosh-Pro on macOS, specifically the "RunAsNode" fuse enabled, allows a local attacker with unprivileged access to execute arbitrary code that inherits Mosh-Pro TCC (Transparency, Consent, and Control) permissions. Acquired resource access is limited to previously granted permissions by the user. Accessing other resources beyond previously granted TCC permissions will prompt the user for approval in the name of Mosh-Pro, potentially disguising attacker's malicious intent. This issue was detected in 1.3.2 version of Mosh-Pro. Since authors did not respond to messages from CNA, patching status is unknown.	N/A	More Details
CVE-2025-38676	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Avoid stack buffer overflow from kernel cmdline While the kernel command line is considered trusted in most environments, avoid writing 1 byte past the end of "acpiid" if the "str" argument is maximum length.	N/A	More Details
CVE-2025-57768	Phproject is a high performance full-featured project management system. From 1.8.0 to before 1.8.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Planned Hours field when creating a new project. When sending a POST request to /issues/new/, the value provided in the Planned Hours field is included in the server response without any HTML encoding or sanitization. Because of this, an attacker can craft a malicious payload such as <script>alert(1)</script> and include it in the planned_hours parameter. The server reflects the input directly in the HTML of the project creation page, causing the browser to interpret and execute it. This vulnerability is fixed in 1.8.3.	N/A	More Details
CVE-2025-54174	QuickCMS is vulnerable to Cross-Site Request Forgery in article creation functionality. Malicious attacker can craft special website, which when visited by the admin, will automatically send a POST request creating a malicious article with content defined by the attacker. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-29901	A NULL pointer dereference vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.4933 and later	N/A	More Details
CVE-2025-57751	pyLoad is the free and open-source Download Manager written in pure Python. The jk parameter is received in pyLoad CNL Blueprint. Due to the lack of jk parameter verification, the jk parameter input by the user is directly determined as dykpy.evaljs(), resulting in the server CPU being fully occupied and the web-ui becoming unresponsive. This vulnerability is fixed in 0.5.0b3.dev92.	N/A	More Details

CVE-2010-10015	AOL versions up to and including 9.5 includes an ActiveX control (Phobos.dll) that exposes a method called Import() via the Phobos.Playlist COM object. This method is vulnerable to a stack-based buffer overflow when provided with an excessively long string argument. Exploitation allows remote attackers to execute arbitrary code in the context of the user, but only when the malicious HTML file is opened locally, due to the control not being marked safe for scripting or initialization. AOL remains an active and supported brand offering services like AOL Mail and AOL Desktop Gold, but the legacy AOL 9.5 desktop software—specifically the version containing the vulnerable Phobos.dll ActiveX control—is long discontinued and no longer maintained.	N/A	More Details
CVE-2010-20109	Barracuda products, confirmed in Spam & Virus Firewall, SSL VPN, and Web Application Firewall versions prior to October 2010, contain a path traversal vulnerability in the view_help.cgi endpoint. The locale parameter fails to properly sanitize user input, allowing attackers to inject traversal sequences and null-byte terminators to access arbitrary files on the underlying system. By exploiting this flaw, unauthenticated remote attackers can retrieve sensitive configuration files such as /mail/snapshot/config.snapshot, potentially exposing credentials, internal settings, and other critical data.	N/A	More Details
CVE-2010-20111	Digital Music Pad v8.2.3.3.4 contains a stack-based buffer overflow vulnerability in its playlist file parser. When opening a .pls file containing an excessively long string in the File1 field, the application fails to properly validate input length, resulting in corruption of the Structured Exception Handler (SEH) on the stack. This flaw may allow an attacker to control execution flow when the file is opened, potentially leading to arbitrary code execution.	N/A	More Details
CVE-2010-20112	Amlib's NetOpacs webquery.dll contains a stack-based buffer overflow vulnerability triggered by improper handling of HTTP GET parameters. Specifically, the application fails to enforce bounds on input supplied to the app parameter, allowing excessive data to overwrite memory structures including the Structured Exception Handler (SEH). Additionally, malformed parameter names followed by an equals sign may result in unintended control flow behavior. This vulnerability is exposed through IIS and affects legacy Windows deployments	N/A	More Details
CVE-2010-20119	CommuniCrypt Mail versions up to and including 1.16 contains a stack-based buffer overflow vulnerability in its ANSMTP.dll and AOSMTP.dll ActiveX controls, specifically within the AddAttachments() method. This method fails to properly validate the length of input strings, allowing data to exceed the bounds of a fixed-size stack buffer. When invoked with an overly long string, the control can corrupt adjacent memory structures, including exception handlers, leading to potential control flow disruption.	N/A	More Details
CVE-2025-29992	Mahara before 24.04.9 exposes database connection information if the database becomes unreachable, e.g., due to the database server being temporarily down or too busy.	N/A	More Details
CVE-2025-50753	Mitrastar GPT-2741GNAC-N2 devices are provided with access through ssh into a restricted default shell.The command "deviceinfo show file" is supposed to be used from restricted shell to show files and directories. By providing " /bin/sh" (quotes included) to the argument of this command will drop a root shell.	N/A	More Details
CVE-2025-55526	n8n-workflows Main Commit ee25413 allows attackers to execute a directory traversal via the download_workflow function within api_server.py	N/A	More Details
CVE-2025-57810	jsPDF is a library to generate PDFs in JavaScript. Prior to 3.0.2, user control of the first argument of the addImage method results in CPU utilization and denial of service. If given the possibility to pass unsanitized image data or URLs to the addImage method, a user can provide a harmful PNG file that results in high CPU utilization and denial of service. The vulnerability was fixed in jsPDF 3.0.2.	N/A	More Details
CVE-2025-57748	Rejected reason: Not used	N/A	More Details
CVE-2025-50976	IPFire 2.29 DNS management interface (dns.cgi) fails to properly sanitize user-supplied input in the NAMESERVER, REMARK, and TLS_HOSTNAME query parameters, resulting in a reflected cross-site scripting (XSS) vulnerability.	N/A	More Details
CVE-2025-9491	Microsoft Windows LNK File UI Misrepresentation Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Windows. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of .LNK files. Crafted data in an .LNK file can cause hazardous content in the file to be invisible to a user who inspects the file via the Windows-provided user interface. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-25373.	N/A	More Details
CVE-2025-57425	A Stored Cross-Site Scripting (XSS) vulnerability in SourceCodester FAQ Management System 1.0 allows an authenticated attacker to inject malicious JavaScript into the 'question' and 'answer' fields via the update-faq.php endpoint.	N/A	More Details
CVE-2025-52184	Cross Site Scripting vulnerability in Helpy.io v.2.8.0 allows a remote attacker to escalate privileges via the New Topic Ticket funtion.	N/A	More Details
CVE-2025-50974	The Calamaris log exporter CGI (/cgi-bin/logs.cgi/calamaris.dat) in IPFire 2.29 does not properly sanitize user-supplied input before incorporating parameter values into a shell command. An unauthenticated remote attacker can inject arbitrary OS commands by embedding shell metacharacters in any of the following parameters BYTE_UNIT, DAY_BEGIN, DAY_END, HIST_LEVEL, MONTH_BEGIN, MONTH_END, NUM_CONTENT, NUM_DOMAINS, NUM_HOSTS, NUM_URLS, PERF_INTERVAL, YEAR_BEGIN, YEAR_END.	N/A	More Details
CVE-2025-53522	Movable Type contains an issue with use of less trusted source. If exploited, tampered email to reset a password may be sent by a remote unauthenticated attacker.	N/A	More Details
CVE-2025-7969	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in markdown-it allows Cross-Site Scripting (XSS). This vulnerability is associated with program files lib/renderer.mjs. This issue affects markdown-it: 14.1.0.	N/A	More Details
CVE-2025-55706	URL redirection to untrusted site ('Open Redirect') issue exists in Movable Type. If this vulnerability is exploited, an invalid parameter may be inserted into the password reset page, which may lead to redirection to an arbitrary URL.	N/A	More Details
CVE-2025-8424	Improper access control on the NetScaler Management Interface in NetScaler ADC and NetScaler Gateway when an attacker can get access to the appliance NSIP, Cluster Management IP or local GSLB Site IP or SNIP with Management Access	N/A	More Details

CVE-2025-52218	SelectZero Data Observability Platform before 2025.5.2 is vulnerable to Content Spoofing / Text Injection. Improper sanitization of unspecified parameters allows attackers to inject arbitrary text or limited HTML into the login page.	N/A	More Details
CVE-2025-52217	SelectZero Data Observability Platform before 2025.5.2 is vulnerable to HTML Injection. Legacy UI fields improperly handle user-supplied input, allowing injection of arbitrary HTML.	N/A	More Details
CVE-2025-43754	Username enumeration vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows attackers to determine if an account exist in the application by inspecting the server processing time of the login request.	N/A	More Details
CVE-2025-25737	Kapsch TrafficCom RIS-9160 & RIS-9260 Roadside Units (RSUs) v3.2.0.829.23, v3.8.0.1119.42, and v4.6.0.1211.28 were discovered to lack secure password requirements for its BIOS Supervisor and User accounts, allowing attackers to bypass authentication via a bruteforce attack.	N/A	More Details
CVE-2025-25736	Kapsch TrafficCom RIS-9260 RSU LEO v3.2.0.829.23, v3.8.0.1119.42, and v4.6.0.1211.28 were discovered to contain Android Debug Bridge (ADB) pre-installed (/mnt/c3platpersistent/opt/platform-tools/adb) and enabled by default, allowing unauthenticated root shell access to the cellular modem via the default 'kapsch' user.	N/A	More Details
CVE-2025-25735	Kapsch TrafficCom RIS-9160 & RIS-9260 Roadside Units (RSUs) v3.2.0.829.23, v3.8.0.1119.42, and v4.6.0.1211.28 were discovered to lack SPI Protected Range Registers (PRRs), allowing attackers with software running on the system to modify SPI flash in real-time.	N/A	More Details
CVE-2025-25734	Kapsch TrafficCom RIS-9160 & RIS-9260 Roadside Units (RSUs) v3.2.0.829.23, v3.8.0.1119.42, and v4.6.0.1211.28 was discovered to contain an unauthenticated EFI shell which allows attackers to execute arbitrary code or escalate privileges during the boot process.	N/A	More Details
CVE-2024-39335	Supported versions of Mahara 24.04 before 24.04.1 and 23.04 before 23.04.6 are vulnerable to information being disclosed to an institution administrator under certain conditions via the 'Current submissions' page: Administration -> Groups -> Submissions.	N/A	More Details
CVE-2025-5302	A denial of service vulnerability exists in the JSONReader component of the run-llama/llama_index repository, specifically in version v0.12.37. The vulnerability is caused by uncontrolled recursion when parsing deeply nested JSON files, which can lead to Python hitting its maximum recursion depth limit. This results in high resource consumption and potential crashes of the Python process. The issue is resolved in version 0.12.38.	N/A	More Details
CVE-2011-10022	SPlayer version 3.7 and earlier is vulnerable to a stack-based buffer overflow when processing HTTP responses containing an overly long Content-Type header. The vulnerability occurs due to improper bounds checking on the header value, allowing an attacker to overwrite the Structured Exception Handler (SEH) and execute arbitrary code. Exploitation requires the victim to open a media file that triggers an HTTP request to a malicious server, which responds with a crafted Content-Type header.	N/A	More Details
CVE-2025-54175	QuickCMS.EXT is vulnerable to Reflected XSS in sFileName parameter in thumbnail viewer functionality. An attacker can craft a malicious URL that results in arbitrary JavaScript execution in the victim's browser when opened. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.8 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-57832	Rejected reason: Not used	N/A	More Details
CVE-2025-57826	Rejected reason: Not used	N/A	More Details
CVE-2025-57827	Rejected reason: Not used	N/A	More Details
CVE-2025-57828	Rejected reason: Not used	N/A	More Details
CVE-2025-57829	Rejected reason: Not used	N/A	More Details
CVE-2025-53363	dpanel is an open source server management panel written in Go. In versions 1.2.0 through 1.7.2, dpanel allows authenticated users to read arbitrary files from the server via the /api/app/compose/get-from-uri API endpoint. The vulnerability exists in the GetFromUri function in app/application/http/controller/compose.go, where the uri parameter is passed directly to os.ReadFile without proper validation or access control. A logged-in attacker can exploit this flaw to read sensitive files from the host system, leading to information disclosure. No patched version is available as of this writing.	N/A	More Details
CVE-2025-57830	Rejected reason: Not used	N/A	More Details
CVE-2025-57831	Rejected reason: Not used	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: drop UFO packets in udp_rcv_segment() When sending a packet with virtio_net_hdr to tun device, if the gso_type in virtio_net_hdr is SKB_GSO_UDP and the gso_size is less than udphdr size, below crash may happen. ------------[cut here]------------ kernel BUG at net/core/skbuff.c:4572! Oops: invalid opcode: 0000 [#1] SMP NOPTI CPU: 0 UID: 0 PID: 62 Comm: mytest Not tainted 6.16.0-rc7 #203 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:skb_pull_rcsum+0x8e/0xa0 Code: 00 00 5b c3 cc cc cc cc 8b 93 88 00 00 00 f7 da e8 37 44 38 00 f7 d8 89 83 88 00 00 00 48 8b 83 c8 00 00 00 5b c3 cc cc cc cc <0f> 0b 0f 0b 66 66 2e 0f 1f 84 00 000 RSP: 0018:ffffc900001fba38		

CVE-2025-38622	EFLAGS: 00000297 RAX: 0000000000000004 RBX: ffff8880040c1000 RCX: ffffc900001fb948 RDX: ffff888003e6d700 RSI: 0000000000000008 RDI: ffff88800411a062 RBP: ffff8880040c1000 R08: 0000000000000000 R09: 0000000000000001 R10: ffff888003606c00 R11: 0000000000000001 R12: 0000000000000000 R13: ffff888004060900 R14: ffff888004050000 R15: ffff888004060900 FS: 000000002406d3c0(0000) GS:ffff888084a19000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000040 CR3: 0000000004007000 CR4: 00000000000006f0 Call Trace: <TASK> udp_queue_rcv_one_skb+0x176/0x4b0 net/ipv4/udp.c:2445 udp_queue_rcv_skb+0x155/0x1f0 net/ipv4/udp.c:2475 udp_unicast_rcv_skb+0x71/0x90 net/ipv4/udp.c:2626 __udp4_lib_rcv+0x433/0xb00 net/ipv4/udp.c:2690 ip_protocol_deliver_rcu+0xa6/0x160 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x72/0x90 net/ipv4/ip_input.c:233 ip_sublist_rcv_finish+0x5f/0x70 net/ipv4/ip_input.c:579 ip_sublist_rcv+0x122/0x1b0 net/ipv4/ip_input.c:636 ip_list_rcv+0xf7/0x130 net/ipv4/ip_input.c:670 __netif_receive_skb_list_core+0x21d/0x240 net/core/dev.c:6067 netif_receive_skb_list_internal+0x186/0x2b0 net/core/dev.c:6210 napi_complete_done+0x78/0x180 net/core/dev.c:6580 tun_get_user+0xa63/0x1120 drivers/net/tun.c:1909 tun_chr_write_iter+0x65/0xb0 drivers/net/tun.c:1984 vfs_write+0x300/0x420 fs/read_write.c:593 ksys_write+0x60/0xd0 fs/read_write.c:686 do_syscall_64+0x50/0x1c0 arch/x86/entry/syscall_64.c:63 </TASK> To trigger gso segment in udp_queue_rcv_skb(), we should also set option UDP_ENCAP_ESPINUDP to enable udp_sk(sk)->encap_rcv. When the encap_rcv hook return 1 in udp_queue_rcv_one_skb(), udp_csum_pull_header() will try to pull udphdr, but the skb size has been segmented to gso size, which leads to this crash. Previous commit cf329aa42b66 ("udp: cope with UDP GRO packet misdirection") introduces segmentation in UDP receive path only for GRO, which was never intended to be used for UFO, so drop UFO packets in udp_rcv_segment().	N/A	More Details
CVE-2025-43751	User enumeration vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14, 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10 and 7.4 GA through update 92 allows remote attackers to determine if an account exist in the application via the create account page.	N/A	More Details
CVE-2025-54923	CWE-502: Deserialization of Untrusted Data vulnerability exists that could cause remote code execution and compromise of system integrity when authenticated users send crafted data to a network-exposed service that performs unsafe deserialization.	N/A	More Details
CVE-2025-38675	In the Linux kernel, the following vulnerability has been resolved: xfrm: state: initialize state_ptrs earlier in xfrm_state_find In case of preemption, xfrm_state_look_at will find a different pcpu_id and look up states for that other CPU. If we matched a state for CPU2 in the state_cache while the lookup started on CPU1, we will jump to "found", but the "best" state that we got will be ignored and we will enter the "acquire" block. This block uses state_ptrs, which isn't initialized at this point. Let's initialize state_ptrs just after taking rcu_read_lock. This will also prevent a possible misuse in the future, if someone adjusts this function.	N/A	More Details
CVE-2025-38674	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/prime: Use dma_buf from GEM object instance" This reverts commit f83a9b8c7fd0557b0c50784bfdc1bbe9140c9bf8. The dma_buf field in struct drm_gem_object is not stable over the object instance's lifetime. The field becomes NULL when user space releases the final GEM handle on the buffer object. This resulted in a NULL-pointer deref. Workarounds in commit 5307dce878d4 ("drm/gem: Acquire references on GEM handles for framebuffers") and commit f6bfc9afc751 ("drm/framebuffer: Acquire internal references on GEM handles") only solved the problem partially. They especially don't work for buffer objects without a DRM framebuffer associated. Hence, this revert to going back to using .import_attach->dmabuf. v3: - cc stable	N/A	More Details
CVE-2025-38673	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/gem-framebuffer: Use dma_buf from GEM object instance" This reverts commit cce16fcd7446dcff7480cd9d2b6417075ed81065. The dma_buf field in struct drm_gem_object is not stable over the object instance's lifetime. The field becomes NULL when user space releases the final GEM handle on the buffer object. This resulted in a NULL-pointer deref. Workarounds in commit 5307dce878d4 ("drm/gem: Acquire references on GEM handles for framebuffers") and commit f6bfc9afc751 ("drm/framebuffer: Acquire internal references on GEM handles") only solved the problem partially. They especially don't work for buffer objects without a DRM framebuffer associated. Hence, this revert to going back to using .import_attach->dmabuf. v3: - cc stable	N/A	More Details
CVE-2025-38672	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/gem-dma: Use dma_buf from GEM object instance" This reverts commit e8afa1557f4f963c9a511bd2c6074a941c308685. The dma_buf field in struct drm_gem_object is not stable over the object instance's lifetime. The field becomes NULL when user space releases the final GEM handle on the buffer object. This resulted in a NULL-pointer deref. Workarounds in commit 5307dce878d4 ("drm/gem: Acquire references on GEM handles for framebuffers") and commit f6bfc9afc751 ("drm/framebuffer: Acquire internal references on GEM handles") only solved the problem partially. They especially don't work for buffer objects without a DRM framebuffer associated. Hence, this revert to going back to using .import_attach->dmabuf. v3: - cc stable	N/A	More Details
CVE-2025-38671	In the Linux kernel, the following vulnerability has been resolved: i2c: qup: jump out of the loop in case of timeout Original logic only sets the return value but doesn't jump out of the loop if the bus is kept active by a client. This is not expected. A malicious or buggy i2c client can hang the kernel in this case and should be avoided. This is observed during a long time test with a PCA953x GPIO extender. Fix it by changing the logic to not only sets the return value, but also jumps out of the loop and return to the caller with -ETIMEDOUT.	N/A	More Details
CVE-2025-38670	In the Linux kernel, the following vulnerability has been resolved: arm64/entry: Mask DAIF in cpu_switch_to(), call_on_irq_stack() `cpu_switch_to()` and `call_on_irq_stack()` manipulate SP to change to different stacks along with the Shadow Call Stack if it is enabled. Those two stack changes cannot be done atomically and both functions can be interrupted by SErrors or Debug Exceptions which, though unlikely, is very much broken : if interrupted, we can end up with mismatched stacks and Shadow Call Stack leading to clobbered stacks. In `cpu_switch_to()`, it can happen when SP_EL0 points to the new task, but x18 stills points to the old task's SCS. When the interrupt handler tries to save the task's SCS pointer, it will save the old task SCS pointer (x18) into the new task struct (pointed to by SP_EL0), clobbering it. In `call_on_irq_stack()`, it can happen when switching from the task stack to the IRQ stack and when switching back. In both cases, we can be interrupted when the SCS pointer points to the IRQ SCS, but SP points to the task stack. The nested interrupt handler pushes its return addresses on the IRQ SCS. It then detects that SP points to the task stack, calls `call_on_irq_stack()` and clobbers the task SCS pointer with the IRQ SCS pointer, which it will also use ! This leads to tasks returning to addresses on the wrong SCS, or even on the IRQ SCS, triggering kernel panics via CONFIG_VMAP_STACK or FPAC if enabled. This is possible on a default config, but unlikely. However, when enabling CONFIG_ARM64_PSEUDO_NMI, DAIF is unmasked and instead the GIC is responsible for filtering what interrupts the CPU should receive based on priority. Given the goal of emulating NMIs, pseudo-NMIs can be received by the CPU even in `cpu_switch_to()` and `call_on_irq_stack()`, possibly *very* frequently depending on the system configuration and workload, leading to unpredictable kernel panics. Completely mask DAIF in `cpu_switch_to()` and restore it when returning. Do the same in `call_on_irq_stack()`, but restore and mask around the branch. Mask DAIF even if CONFIG_SHADOW_CALL_STACK is not enabled for consistency of behaviour between all configurations. Introduce and use an assembly macro for saving and masking DAIF, as the existing one saves but only masks IF.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/gem-shmem: Use dma_buf from GEM object instance" This reverts commit 1a148af06000e545e714fe3210af3d77ff903c11. The dma_buf field in struct drm_gem_object is not stable over the object instance's lifetime. The field becomes NULL when user space releases the final GEM handle on the buffer object. This resulted in a NULL-pointer deref. Workarounds in commit 5307dce878d4 ("drm/gem: Acquire references on GEM handles for framebuffers") and commit	N/A	More Details

38669	f6bfc9afc751 ("drm/framebuffer: Acquire internal references on GEM handles") only solved the problem partially. They especially don't work for buffer objects without a DRM framebuffer associated. Hence, this revert to going back to using .import_attach->dmabuf. v3: - cc stable		
CVE-2025-38668	In the Linux kernel, the following vulnerability has been resolved: regulator: core: fix NULL dereference on unbind due to stale coupling data Failing to reset coupling_desc.n_coupled after freeing coupled_rdevs can lead to NULL pointer dereference when regulators are accessed post-unbind. This can happen during runtime PM or other regulator operations that rely on coupling metadata. For example, on ridesx4, unbinding the 'reg-dummy' platform device triggers a panic in regulator_lock_recursive() due to stale coupling state. Ensure n_coupled is set to 0 to prevent access to invalid pointers.	N/A	More Details
CVE-2025-57825	Rejected reason: Not used	N/A	More Details
CVE-2025-57824	Rejected reason: Not used	N/A	More Details
CVE-2025-38621	In the Linux kernel, the following vulnerability has been resolved: md: make rdev_addable usable for rcu mode Our testcase trigger panic: BUG: kernel NULL pointer dereference, address: 00000000000000e0 ... Oops: Oops: 0000 [#1] SMP NOPTI CPU: 2 UID: 0 PID: 85 Comm: kworker/2:1 Not tainted 6.16.0+ #94 PREEMPT(none) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Workqueue: md_misc md_start_sync RIP: 0010:rdev_addable+0x4d/0xf0 ... Call Trace: <TASK> md_start_sync+0x329/0x480 process_one_work+0x226/0x6d0 worker_thread+0x19e/0x340 kthread+0x10f/0x250 ret_from_fork+0x14d/0x180 ret_from_fork_asm+0x1a/0x30 </TASK> Modules linked in: raid10 CR2: 00000000000000e0 ---[end trace 0000000000000000]--- RIP: 0010:rdev_addable+0x4d/0xf0 md_spares_need_change in md_start_sync will call rdev_addable which protected by rcu_read_lock/rcu_read_unlock. This rcu context will help protect rdev won't be released, but rdev->mddev will be set to NULL before we call synchronize_rcu in md_kick_rdev_from_array. Fix this by using READ_ONCE and check does rdev->mddev still alive.	N/A	More Details
CVE-2025-38620	In the Linux kernel, the following vulnerability has been resolved: zloop: fix KASAN use-after-free of tag set When a zoned loop device, or zloop device, is removed, KASAN enabled kernel reports "BUG KASAN use-after-free" in blk_mq_free_tag_set(). The BUG happens because zloop_ctl_remove() calls put_disk(), which invokes zloop_free_disk(). The zloop_free_disk() frees the memory allocated for the zlo pointer. However, after the memory is freed, zloop_ctl_remove() calls blk_mq_free_tag_set(&zlo->tag_set), which accesses the freed zlo. Hence the KASAN use-after-free. zloop_ctl_remove() put_disk(zlo->disk) put_device() kobject_put() ... zloop_free_disk() kvfree(zlo) blk_mq_free_tag_set(&zlo->tag_set) To avoid the BUG, move the call to blk_mq_free_tag_set(&zlo->tag_set) from zloop_ctl_remove() into zloop_free_disk(). This ensures that the tag_set is freed before the call to kvfree(zlo).	N/A	More Details
CVE-2025-43759	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows admin users of a virtual instance to add pages that are not in the default/main virtual instance, then any tenant can create a list of all other tenants.	N/A	More Details
CVE-2025-43758	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.5, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15 and 7.4 GA through update 92 allows unauthenticated users (guests) to access via URL files uploaded by object entry and stored in document_library	N/A	More Details
CVE-2009-10006	UFO: Alien Invasion versions up to and including 2.2.1 contain a buffer overflow vulnerability in its built-in IRC client component. When the client connects to an IRC server and receives a crafted numeric reply (specifically a 001 message), the application fails to properly validate the length of the response string. This results in a stack-based buffer overflow, which may corrupt control flow structures and allow arbitrary code execution. The vulnerability is triggered during automatic IRC connection handling and does not require user interaction beyond launching the game.	N/A	More Details
CVE-2025-43746	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.2, 2025.Q1.0 through 2025.Q1.10, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.18 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code via _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_portletNamespace and _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_namespace parameter.	N/A	More Details
CVE-2025-43760	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4, 2024.Q4.0 through 2024.Q4.6, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.20 and 7.4 GA through update 92 allows an remote authenticated attacker to inject JavaScript into the PortalUtil.escapeRedirect	N/A	More Details
CVE-2025-43757	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.2, 2025.Q1.0 through 2025.Q1.14, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.18 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code via _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_definition parameter.	N/A	More Details
CVE-2024-58239	In the Linux kernel, the following vulnerability has been resolved: tls: stop recv() if initial process_rx_list gave us non-DATA If we have a non-DATA record on the rx_list and another record of the same type still on the queue, we will end up merging them: - process_rx_list copies the non-DATA record - we start the loop and process the first available record since it's of the same type - we break out of the loop since the record was not DATA Just check the record type and jump to the end in case process_rx_list did some work.	N/A	More Details
CVE-2025-55745	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. Versions 0.3.0 and prior are vulnerable to CSV injection, also known as formula injection, in the Quick Export feature. This vulnerability allows attackers to inject malicious content into exported CSV files. When the CSV file is opened in spreadsheet applications such as Microsoft Excel, the malicious input may be interpreted as a formula or command, potentially resulting in the execution of arbitrary code on the victim's device. Successful exploitation can lead to remote code execution, including the establishment of a reverse shell. Users are advised to upgrade to version 0.3.1 or later.	N/A	More Details
CVE-2025-5115	In Eclipse Jetty, versions <=9.4.57, <=10.0.25, <=11.0.25, <=12.0.21, <=12.1.0.alpha2, an HTTP/2 client may trigger the server to send RST_STREAM frames, for example by sending frames that are malformed or that should not be sent in a particular stream state, therefore forcing the server to consume resources such as CPU and memory. For example, a client can open a stream and then send WINDOW_UPDATE frames with window size increment of 0, which is illegal. Per specification https://www.rfc-editor.org/rfc/rfc9113.html#name-window_update , the server should send a RST_STREAM frame. The client can now open another stream and send another bad WINDOW_UPDATE, therefore causing the server to consume more resources than necessary, as this case does not exceed the max number of concurrent streams, yet the client is able to create an enormous amount of streams in a short period of time. The attack can be performed with other conditions (for example, a DATA frame for a closed stream) that cause the server to send a RST_STREAM frame. Links: * https://github.com/jetty/jetty.project/security/advisories/GHSA-mmxm-8w33-wc4h	N/A	More Details

CVE-2025-38616	In the Linux kernel, the following vulnerability has been resolved: tls: handle data disappearing from under the TLS ULP TLS expects that it owns the receive queue of the TCP socket. This cannot be guaranteed in case the reader of the TCP socket entered before the TLS ULP was installed, or uses some non-standard read API (eg. zerocopy ones). Replace the WARN_ON() and a buggy early exit (which leaves anchor pointing to a freed skb) with real error handling. Wipe the parsing state and tell the reader to retry. We already reload the anchor every time we (re)acquire the socket lock, so the only condition we need to avoid is an out of bounds read (not having enough bytes in the socket for previously parsed record len). If some data was read from under TLS but there's enough in the queue we'll reload and decrypt what is most likely not a valid TLS record. Leading to some undefined behavior from TLS perspective (corrupting a stream? missing an alert? missing an attack?) but no kernel crash should take place.	N/A	More Details
CVE-2025-38617	In the Linux kernel, the following vulnerability has been resolved: net/packet: fix a race in packet_set_ring() and packet_notifier() When packet_set_ring() releases po->bind_lock, another thread can run packet_notifier() and process an NETDEV_UP event. This race and the fix are both similar to that of commit 15fe076edea7 ("net/packet: fix a race in packet_bind() and packet_notifier()"). There too the packet_notifier NETDEV_UP event managed to run while a po->bind_lock critical section had to be temporarily released. And the fix was similarly to temporarily set po->num to zero to keep the socket unhooked until the lock is retaken. The po->bind_lock in packet_set_ring and packet_notifier precede the introduction of git history.	N/A	More Details
CVE-2025-9287	Improper Input Validation vulnerability in cipher-base allows Input Data Manipulation.This issue affects cipher-base: through 1.0.4.	N/A	More Details
CVE-2025-9288	Improper Input Validation vulnerability in sha.js allows Input Data Manipulation.This issue affects sha.js: through 2.4.11.	N/A	More Details
CVE-2025-38618	In the Linux kernel, the following vulnerability has been resolved: vsock: Do not allow binding to VMADDR_PORT_ANY It is possible for a vsock to autobind to VMADDR_PORT_ANY. This can cause a use-after-free when a connection is made to the bound socket. The socket returned by accept() also has port VMADDR_PORT_ANY but is not on the list of unbound sockets. Binding it will result in an extra refcount decrement similar to the one fixed in fcdd2242c023 (vsock: Keep the binding until socket destruction). Modify the check in __vsock_bind_connectible() to also prevent binding to VMADDR_PORT_ANY.	N/A	More Details
CVE-2025-53505	Group-Office versions prior to 6.8.119 and prior to 25.0.20 provided by Intermesh BV contain a path traversal vulnerability. If this vulnerability is exploited, information on the server hosting the product may be exposed.	N/A	More Details
CVE-2025-53504	Group-Office versions prior to 6.8.119 and prior to 25.0.20 provided by Intermesh BV contain a cross-site scripting vulnerability. If this vulnerability is exploited, an arbitrary script may be executed in the user's web browser.	N/A	More Details
CVE-2025-38619	In the Linux kernel, the following vulnerability has been resolved: media: ti: j721e-csi2rx: fix list_del corruption If ti_csi2rx_start_dma() fails in ti_csi2rx_dma_callback(), the buffer is marked done with VB2_BUF_STATE_ERROR but is not removed from the DMA queue. This causes the same buffer to be retried in the next iteration, resulting in a double list_del() and eventual list corruption. Fix this by removing the buffer from the queue before calling vb2_buffer_done() on error. This resolves a crash due to list_del corruption: [37.811243] j721e-csi2rx 30102000.ticsi2rx: Failed to queue the next buffer for DMA [37.832187] slab kmalloc-2k start ffff00000255b000 pointer offset 1064 size 2048 [37.839761] list_del corruption. next->prev should be ffff00000255bc28, but was ffff00000255d428. (next=ffff00000255b428) [37.850799] ------------[cut here]------------ [37.855424] kernel BUG at lib/list_debug.c:65! [37.859876] Internal error: Oops - BUG: 00000000f2000800 [#1] SMP [37.866061] Modules linked in: i2c_dev usb_f_rndis u_ether libcomposite dwc3 udc_core usb_common aes_ce_blk aes_ce_cipher ghash_ce gf128mul sha1_ce cpufreq_dt dwc3_am62 phy_gmii_sel sa2ul [37.882830] CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Not tainted 6.16.0-rc3+ #28 VOLUNTARY [37.890851] Hardware name: Bosch STLA-GSRV2-B0 (DT) [37.895737] pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [37.902703] pc : __list_del_entry_valid_or_report+0xdc/0x114 [37.908390] lr : __list_del_entry_valid_or_report+0xdc/0x114 [37.914059] sp : ffff800080003db0 [37.917375] x29: ffff800080003db0 x28: 0000000000000007 x27: ffff800080e50000 [37.924521] x26: 0000000000000000 x25: ffff0000016abb50 x24: dead000000000122 [37.931666] x23: ffff0000016abb78 x22: ffff0000016ab080 x21: ffff800080003de0 [37.938810] x20: ffff00000255bc00 x19: ffff00000255b800 x18: 000000000000000a [37.945956] x17: 20747562202c3832 x16: 6362353532303030 x15: 0720072007200720 [37.953101] x14: 0720072007200720 x13: 0720072007200720 x12: 00000000ffffffea [37.960248] x11: ffff800080003b18 x10: 00000000ffffefff x9 : ffff800080f5b568 [37.967396] x8 : ffff800080f5b5c0 x7 : 0000000000017fe8 x6 : c0000000ffffefff [37.974542] x5 : ffff00000fea6688 x4 : 0000000000000000 x3 : 0000000000000000 [37.981686] x2 : 0000000000000000 x1 : ffff800080ef2b40 x0 : 000000000000006d [37.988832] Call trace: [37.991281] __list_del_entry_valid_or_report+0xdc/0x114 (P) [37.996959] ti_csi2rx_dma_callback+0x84/0x1c4 [38.001419] udma_vchan_complete+0x1e0/0x344 [38.005705] tasklet_action_common+0x118/0x310 [38.010163] tasklet_action+0x30/0x3c [38.013832] handle_softirqs+0x10c/0x2e0 [38.017761] __do_softirq+0x14/0x20 [38.021256] ____do_softirq+0x10/0x20 [38.024931] call_on_irq_stack+0x24/0x60 [38.028873] do_softirq_own_stack+0x1c/0x40 [38.033064] __irq_exit_rcu+0x130/0x15c [38.036909] irq_exit_rcu+0x10/0x20 [38.040403] el1_interrupt+0x38/0x60 [38.043987] el1h_64_irq_handler+0x18/0x24 [38.048091] el1h_64_irq+0x6c/0x70 [38.051501] default_idle_call+0x34/0xe0 (P) [38.055783] do_idle+0x1f8/0x250 [38.059021] cpu_startup_entry+0x34/0x3c [38.062951] rest_init+0xb4/0xc0 [38.066186] console_on_rootfs+0x0/0x6c [38.070031] __primary_switched+0x88/0x90 [38.074059] Code: b00037e0 91378000 f9400462 97e9bf49 (d4210000) [38.080168] ---[end trace 0000000000000000]--- [38.084795] Kernel panic - not syncing: Oops - BUG: Fatal exception in interrupt [38.092197] SMP: stopping secondary CPUs [38.096139] Kernel Offset: disabled [38.099631] CPU features: 0x0000,00002000,02000801,0400420b [38.105202] Memory Limit: none [38.108260] ---[end Kernel panic - not syncing: Oops - BUG: Fatal exception in interrupt]---	N/A	More Details
CVE-2025-38667	In the Linux kernel, the following vulnerability has been resolved: iio: fix potential out-of-bound write The buffer is set to 20 characters. If a caller write more characters, count is truncated to the max available space in "simple_write_to_buffer". To protect from OoB access, check that the input size fit into buffer and add a zero terminator after copy to the end of the copied data.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: appletalk: Fix use-after-free in AARP proxy probe The AARP proxy-probe routine (aarp_proxy_probe_network) sends a probe, releases the aarp_lock, sleeps, then re-acquires the lock. During that window an expire timer thread (__aarp_expire_timer) can remove and kfree() the same entry, leading to a use-after-free. race condition: cpu 0 | cpu 1 atalk_sendmsg() | atif_proxy_probe_device() aarp_send_ddp() | aarp_proxy_probe_network() mod_timer() | lock(aarp_lock) // LOCK!! timeout around 200ms | alloc(aarp_entry) and then call | proxies[hash] = aarp_entry aarp_expire_timeout() | aarp_send_probe() | unlock(aarp_lock) // UNLOCK!! lock(aarp_lock) // LOCK!! | msleep(100); __aarp_expire_timer(&proxies[ct]) | free(aarp_entry) | unlock(aarp_lock) // UNLOCK!! | | lock(aarp_lock) // LOCK!! | UAF aarp_entry !! == BUG: KASAN: slab-use-after-free in aarp_proxy_probe_network+0x560/0x630 net/appletalk/aarp.c:493 Read of size 4 at addr ffff8880123aa360 by task repro/13278 CPU: 3 UID: 0 PID: 13278 Comm: repro Not tainted 6.15.2 #3 PREEMPT(full) Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1b0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline]		

CVE-2025-38666	print_report+0xc1/0x630 mm/kasan/report.c:521 kasan_report+0xca/0x100 mm/kasan/report.c:634 aarp_proxy_probe_network+0x560/0x630 net/appletalk/aarp.c:493 atif_proxy_probe_device net/appletalk/ddp.c:332 [inline] atif_ioctl+0xb58/0x16c0 net/appletalk/ddp.c:857 atalk_ioctl+0x198/0x2f0 net/appletalk/ddp.c:1818 sock_do_ioctl+0xdc/0x260 net/socket.c:1190 sock_ioctl+0x239/0x6a0 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+0x194/0x200 fs/ioctl.c:892 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcb/0x250 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Allocated: aarp_alloc net/appletalk/aarp.c:382 [inline] aarp_proxy_probe_network+0xd8/0x630 net/appletalk/aarp.c:468 atif_proxy_probe_device net/appletalk/ddp.c:332 [inline] atif_ioctl+0xb58/0x16c0 net/appletalk/ddp.c:857 atalk_ioctl+0x198/0x2f0 net/appletalk/ddp.c:1818 Freed: kfree+0x148/0x4d0 mm/slub.c:4841 __aarp_expire net/appletalk/aarp.c:90 [inline] __aarp_expire_timer net/appletalk/aarp.c:261 [inline] aarp_expire_timeout+0x480/0x6e0 net/appletalk/aarp.c:317 The buggy address belongs to the object at ffff8880123aa300 which belongs to the cache kmalloc-192 of size 192 The buggy address is located 96 bytes inside of freed 192-byte region [ffff8880123aa300, ffff8880123aa3c0) Memory state around the buggy address: ffff8880123aa200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff8880123aa280: 00 00 00 00 fc fc fc fc fc fc fc fc fc fc fc fc >ffff8880123aa300: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8880123aa380: fb fb fb fb fb fb fb fb fc fc fc fc fc fc fc fc ffff8880123aa400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ==========	N/A	More Details
CVE-2025-38665	In the Linux kernel, the following vulnerability has been resolved: can: netlink: can_changelink(): fix NULL pointer deref of struct can_priv::do_set_mode Andrei Lalaev reported a NULL pointer deref when a CAN device is restarted from Bus Off and the driver does not implement the struct can_priv::do_set_mode callback. There are 2 code path that call struct can_priv::do_set_mode: - directly by a manual restart from the user space, via can_changelink() - delayed automatic restart after bus off (deactivated by default) To prevent the NULL pointer deference, refuse a manual restart or configure the automatic restart delay in can_changelink() and report the error via extack to user space. As an additional safety measure let can_restart() return an error if can_priv::do_set_mode is not set instead of dereferencing it unchecked.	N/A	More Details
CVE-2025-38644	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: reject TDLS operations when station is not associated syzbot triggered a WARN in ieee80211_tdls_oper() by sending NL80211_TDLS_ENABLE_LINK immediately after NL80211_CMD_CONNECT, before association completed and without prior TDLS setup. This left internal state like sdata->u.mgd.tdls_peer uninitialized, leading to a WARN_ON() in code paths that assumed it was valid. Reject the operation early if not in station mode or not associated.	N/A	More Details
CVE-2025-38642	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix WARN_ON for monitor mode on some devices On devices without WANT_MONITOR_VIF (and probably without channel context support) we get a WARN_ON for changing the per-link setting of a monitor interface. Since we already skip AP_VLAN interfaces and MONITOR with WANT_MONITOR_VIF and/or NO_VIRTUAL_MONITOR should update the settings, catch this in the link change code instead of the warning.	N/A	More Details
CVE-2025-38641	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: Fix potential NULL dereference on kmalloc failure Avoid potential NULL pointer dereference by checking the return value of kmalloc and handling allocation failure properly.	N/A	More Details
CVE-2025-38640	In the Linux kernel, the following vulnerability has been resolved: bpf: Disable migration in nf_hook_run_bpf(). syzbot reported that the netfilter bpf prog can be called without migration disabled in xmit path. Then the assertion in __bpf_prog_run() fails, triggering the splat below. [0] Let's use bpf_prog_run_pin_on_cpu() in nf_hook_run_bpf(). [0]: BUG: assuming non migratable context at ./include/linux/filter.h:703 in_atomic(): 0, irqs_disabled(): 0, migration_disabled() 0 pid: 5829, name: sshd-session 3 locks held by sshd-session/5829: #0: ffff88807b4e4218 (sk_lock-AF_INET){+.+.}-{0:0}, at: lock_sock include/net/sock.h:1667 [inline] #0: ffff88807b4e4218 (sk_lock-AF_INET){+.+.}-{0:0}, at: tcp_sendmsg+0x20/0x50 net/ipv4/tcp.c:1395 #1: ffffffff8e5c4e00 (rcu_read_lock){....}-{1:3}, at: rcu_lock_acquire include/linux/rcupdate.h:331 [inline] #1: ffffffff8e5c4e00 (rcu_read_lock){....}-{1:3}, at: rcu_read_lock include/linux/rcupdate.h:841 [inline] #1: ffffffff8e5c4e00 (rcu_read_lock){....}-{1:3}, at: __ip_queue_xmit+0x69/0x26c0 net/ipv4/ip_output.c:470 #2: ffffffff8e5c4e00 (rcu_read_lock){....}-{1:3}, at: rcu_lock_acquire include/linux/rcupdate.h:331 [inline] #2: ffffffff8e5c4e00 (rcu_read_lock){....}-{1:3}, at: rcu_read_lock include/linux/rcupdate.h:841 [inline] #2: ffffffff8e5c4e00 (rcu_read_lock){....}-{1:3}, at: nf_hook+0xb2/0x680 include/linux/netfilter.h:241 CPU: 0 UID: 0 PID: 5829 Comm: sshd-session Not tainted 6.16.0-rc6-syzkaller-00002-g155a3c003e55 #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/07/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x16c/0x1f0 lib/dump_stack.c:120 __cant_migrate kernel/sched/core.c:8860 [inline] __cant_migrate+0x1c7/0x250 kernel/sched/core.c:8834 __bpf_prog_run include/linux/filter.h:703 [inline] bpf_prog_run include/linux/filter.h:725 [inline] nf_hook_run_bpf+0x83/0x1e0 net/netfilter/nf_bpf_link.c:20 nf_hook_entry_hookfn include/linux/netfilter.h:157 [inline] nf_hook_slow+0xbb/0x200 net/netfilter/core.c:623 nf_hook+0x370/0x680 include/linux/netfilter.h:272 NF_HOOK_COND include/linux/netfilter.h:305 [inline] ip_output+0x1bc/0x2a0 net/ipv4/ip_output.c:433 dst_output include/net/dst.h:459 [inline] ip_local_out net/ipv4/ip_output.c:129 [inline] __ip_queue_xmit+0x1d7d/0x26c0 net/ipv4/ip_output.c:527 __tcp_transmit_skb+0x2686/0x3e90 net/ipv4/tcp_output.c:1479 tcp_transmit_skb net/ipv4/tcp_output.c:1497 [inline] tcp_write_xmit+0x1274/0x84e0 net/ipv4/tcp_output.c:2838 __tcp_push_pending_frames+0xaf/0x390 net/ipv4/tcp_output.c:3021 tcp_push+0x225/0x700 net/ipv4/tcp.c:759 tcp_sendmsg_locked+0x1870/0x42b0 net/ipv4/tcp.c:1359 tcp_sendmsg+0x2e/0x50 net/ipv4/tcp.c:1396 inet_sendmsg+0xb9/0x140 net/ipv4/af_inet.c:851 sock_sendmsg_nosec net/socket.c:712 [inline] __sock_sendmsg net/socket.c:727 [inline] sock_write_iter+0x4aa/0x5b0 net/socket.c:1131 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x6c7/0x1150 fs/read_write.c:686 ksys_write+0x1f8/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0x4c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fe7d365d407 Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 fa 08 75 de e8 23 ff ff ff RSP:	N/A	More Details
CVE-2025-38639	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_nfacct: don't assume acct name is null-terminated BUG: KASAN: slab-out-of-bounds in .. lib/vsprintf.c:721 Read of size 1 at addr ffff88801eac95c8 by task syz-executor183/5851 [..] string+0x231/0x2b0 lib/vsprintf.c:721 vsnprintf+0x739/0xf00 lib/vsprintf.c:2874 [..] nfacct_mt_checkentry+0xd2/0xe0 net/netfilter/xt_nfacct.c:41 xt_check_match+0x3d1/0xab0 net/netfilter/x_tables.c:523 nfnl_acct_find_get() handles non-null input, but the error printk relied on its presence.	N/A	More Details
CVE-2025-38638	In the Linux kernel, the following vulnerability has been resolved: ipv6: add a retry logic in net6_rt_notify() inet6_rt_notify() can be called under RCU protection only. This means the route could be changed concurrently and rt6_fill_node() could return -EMSGSIZE. Re-size the skb when this happens and retry, removing one WARN_ON() that syzbot was able to trigger: WARNING: CPU: 3 PID: 6291 at net/ipv6/route.c:6342 inet6_rt_notify+0x475/0x4b0 net/ipv6/route.c:6342 Modules linked in: CPU: 3 UID: 0 PID: 6291 Comm: syz.0.77 Not tainted 6.16.0-rc7-syzkaller #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:inet6_rt_notify+0x475/0x4b0 net/ipv6/route.c:6342 Code: fc ff ff e8 6d 52 ea f7 e9 47 fc ff ff 48 8b 7c 24 08 4c 89 04 24 e8 5a 52 ea f7 4c 8b 04 24 e9 94 fd ff ff e8 9c fe 84 f7 90 <0f> 0b 90 e9 bd fd ff ff e8 6e 52 ea f7 e9 bb fb ff ff 48 89 df e8 RSP: 0018:ffffc900035cf1d8 EFLAGS: 00010293 RAX: 0000000000000000 RBX: ffffc900035cf540 RCX: ffffffff8a36e790 RDX: ffff88802f7e8000 RSI: ffffffff8a36e9d4 RDI: 0000000000000005 RBP: ffff88803c230f00 R08: 0000000000000005 R09: 00000000ffffffa6 R10: 00000000ffffffa6 R11: 0000000000000001 R12: 00000000ffffffa6 R13: 0000000000000900 R14: ffff888032ea4100 R15: 0000000000000000 FS: 00007fac7b89a6c0(0000) GS:ffff8880d6a20000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fac7b899f98 CR3: 0000000034b3f000 CR4: 0000000000352ef0 Call Trace: <TASK>	N/A	More Details

	ip6_route_mpath_notify+0xde/0x280 net/ipv6/route.c:5356 ip6_route_multipath_add+0x1181/0x1bd0 net/ipv6/route.c:5536 inet6_rtm_newroute+0xe4/0x1a0 net/ipv6/route.c:5647 rtnetlink_rcv_msg+0x95e/0xe90 net/core/rtnetlink.c:6944 netlink_rcv_skb+0x155/0x420 net/netlink/af_netlink.c:2552 netlink_unicast_kernel net/netlink/af_netlink.c:1320 [inline] netlink_unicast+0x58d/0x850 net/netlink/af_netlink.c:1346 netlink_sendmsg+0x8d1/0xdd0 net/netlink/af_netlink.c:1896 sock_sendmsg_nosec net/socket.c:712 [inline] __sock_sendmsg net/socket.c:727 [inline] ____sys_sendmsg+0xa95/0xc70 net/socket.c:2566 ___sys_sendmsg+0x134/0x1d0 net/socket.c:2620		
CVE-2025-38636	In the Linux kernel, the following vulnerability has been resolved: rv: Use strings in da monitors tracepoints Using DA monitors tracepoints with KASAN enabled triggers the following warning: BUG: KASAN: global-out-of-bounds in do_trace_event_raw_event_event_da_monitor+0xd6/0x1a0 Read of size 32 at addr ffffffffaada8980 by task ... Call Trace: <TASK> [...] do_trace_event_raw_event_event_da_monitor+0xd6/0x1a0 ? __pfx_do_trace_event_raw_event_event_da_monitor+0x10/0x10 ? trace_event_sncid+0x83/0x200 trace_event_sncid+0x163/0x200 [...] The buggy address belongs to the variable: automaton_snep+0x4e0/0x5e0 This is caused by the tracepoints reading 32 bytes __array instead of __string from the automata definition. Such strings are literals and reading 32 bytes ends up in out of bound memory accesses (e.g. the next automaton's data in this case). The error is harmless as, while printing the string, we stop at the null terminator, but it should still be fixed. Use the __string facilities while defining the tracepoints to avoid reading out of bound memory.	N/A	More Details
CVE-2025-38635	In the Linux kernel, the following vulnerability has been resolved: clk: davinci: Add NULL check in davinci_lpsc_clk_register() devm_kasprintf() returns NULL when memory allocation fails. Currently, davinci_lpsc_clk_register() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensuring no resources are left allocated.	N/A	More Details
CVE-2025-38634	In the Linux kernel, the following vulnerability has been resolved: power: supply: cpcap-charger: Fix null check for power_supply_get_by_name In the cpcap_usb_detect() function, the power_supply_get_by_name() function may return `NULL` instead of an error pointer. To prevent potential null pointer dereferences, Added a null check.	N/A	More Details
CVE-2025-38633	In the Linux kernel, the following vulnerability has been resolved: clk: spacemit: mark K1 pll1_d8 as critical The pll1_d8 clock is enabled by the boot loader, and is ultimately a parent for numerous clocks, including those used by APB and AXI buses. Guodong Xu discovered that this clock got disabled while responding to getting -EPROBE_DEFER when requesting a reset controller. The needed clock (CLK_DMA, along with its parents) had already been enabled. To respond to the probe deferral return, the CLK_DMA clock was disabled, and this led to parent clocks also reducing their enable count. When the enable count for pll1_d8 was decremented it became 0, which caused it to be disabled. This led to a system hang. Marking that clock critical resolves this by preventing it from being disabled. Define a new macro CCU_FACTOR_GATE_DEFINE() to allow clock flags to be supplied for a CCU_FACTOR_GATE clock.	N/A	More Details
CVE-2025-38632	In the Linux kernel, the following vulnerability has been resolved: pinmux: fix race causing mux_owner NULL with active mux_usecount commit 5a3e85c3c397 ("pinmux: Use sequential access to access desc->pinmux data") tried to address the issue when two client of the same gpio calls pinctrl_select_state() for the same functionality, was resulting in NULL pointer issue while accessing desc->mux_owner. However, issue was not completely fixed due to the way it was handled and it can still result in the same NULL pointer. The issue occurs due to the following interleaving: cpu0 (process A) cpu1 (process B) pin_request() { pin_free() { mutex_lock() desc->mux_usecount--; //becomes 0 .. mutex_unlock() mutex_lock(desc->mux) desc->mux_usecount++; // becomes 1 desc->mux_owner = owner; mutex_unlock(desc->mux) mutex_lock(desc->mux) desc->mux_owner = NULL; mutex_unlock(desc->mux) This sequence leads to a state where the pin appears to be in use (`mux_usecount == 1`) but has no owner (`mux_owner == NULL`), which can cause NULL pointer on next pin_request on the same pin. Ensure that updates to mux_usecount and mux_owner are performed atomically under the same lock. Only clear mux_owner when mux_usecount reaches zero and no new owner has been assigned.	N/A	More Details
CVE-2025-38631	In the Linux kernel, the following vulnerability has been resolved: clk: imx95-blk-ctl: Fix synchronous abort When enabling runtime PM for clock suppliers that also belong to a power domain, the following crash is thrown: error: synchronous external abort: 0000000096000010 [#1] PREEMPT SMP Workqueue: events_unbound deferred_probe_work_func pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : clk_mux_get_parent+0x60/0x90 lr : clk_core_reparent_orphans_nolock+0x58/0xd8 Call trace: clk_mux_get_parent+0x60/0x90 clk_core_reparent_orphans_nolock+0x58/0xd8 of_clk_add_hw_provider.part.0+0x90/0x100 of_clk_add_hw_provider+0x1c/0x38 imx95_bc_probe+0x2e0/0x3f0 platform_probe+0x70/0xd8 Enabling runtime PM without explicitly resuming the device caused the power domain cut off after clk_register() is called. As a result, a crash happens when the clock hardware provider is added and attempts to access the BLK_CTL register. Fix this by using devm_pm_runtime_enable() instead of pm_runtime_enable() and getting rid of the pm_runtime_disable() in the cleanup path.	N/A	More Details
CVE-2025-38630	In the Linux kernel, the following vulnerability has been resolved: fbdev: imxfb: Check fb_add_videomode to prevent null-ptr-deref fb_add_videomode() can fail with -ENOMEM when its internal kmalloc() cannot allocate a struct fb_modelist. If that happens, the modelist stays empty but the driver continues to register. Add a check for its return value to prevent poteintial null-ptr-deref, which is similar to the commit 17186f1f90d3 ("fbdev: Fix do_register_framebuffer to prevent null-ptr-deref in fb_videomode_to_var").	N/A	More Details
CVE-2025-38629	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb: scarlett2: Fix missing NULL check scarlett2_input_select_ctl_info() sets up the string arrays allocated via kasprintf(), but it misses NULL checks, which may lead to NULL dereference Oops. Let's add the proper NULL check.	N/A	More Details
CVE-2025-38628	In the Linux kernel, the following vulnerability has been resolved: vdpa/mlx5: Fix release of uninitialized resources on error path The commit in the fixes tag made sure that mlx5_vdpa_free() is the single entrypoint for removing the vdpa device resources added in mlx5_vdpa_dev_add(), even in the cleanup path of mlx5_vdpa_dev_add(). This means that all functions from mlx5_vdpa_free() should be able to handle uninitialized resources. This was not the case though: mlx5_vdpa_destroy_mr_resources() and mlx5_cmd_cleanup_async_ctx() were not able to do so. This caused the splat below when adding a vdpa device without a MAC address. This patch fixes these remaining issues: - Makes mlx5_vdpa_destroy_mr_resources() return early if called on uninitialized resources. - Moves mlx5_cmd_init_async_ctx() early on during device addition because it can't fail. This means that mlx5_cmd_cleanup_async_ctx() also can't fail. To mirror this, move the call site of mlx5_cmd_cleanup_async_ctx() in mlx5_vdpa_free(). An additional comment was added in mlx5_vdpa_free() to document the expectations of functions called from this context. Splat: mlx5_core 0000:b5:03.2: mlx5_vdpa_dev_add:3950:(pid 2306) warning: No mac address provisioned? ------------[cut here]------------ WARNING: CPU: 13 PID: 2306 at kernel/workqueue.c:4207 __flush_work+0x9a/0xb0 [...] Call Trace: <TASK> ? __try_to_del_timer_sync+0x61/0x90 ? __timer_delete_sync+0x2b/0x40 mlx5_vdpa_destroy_mr_resources+0x1c/0x40 [mlx5_vdpa] mlx5_vdpa_free+0x45/0x160 [mlx5_vdpa] vdpa_release_dev+0x1e/0x50 [vdpa] device_release+0x31/0x90 kobject_cleanup+0x37/0x130 mlx5_vdpa_dev_add+0x327/0x890 [mlx5_vdpa] vdpa_nl_cmd_dev_add_set_doit+0x2c1/0x4d0 [vdpa] genl_family_rcv_msg_doit+0xd8/0x130 genl_family_rcv_msg+0x14b/0x220 ? __pfx_vdpa_nl_cmd_dev_add_set_doit+0x10/0x10 [vdpa] genl_rcv_msg+0x47/0xa0 ? __pfx_genl_rcv_msg+0x10/0x10 netlink_rcv_skb+0x53/0x100 genl_rcv+0x24/0x40 netlink_unicast+0x27b/0x3b0 netlink_sendmsg+0x1f7/0x430 __sys_sendto+0x1fa/0x210 ? ___pte_offset_map+0x17/0x160 ? next_uptodate_folio+0x85/0x2b0 ? percpu_counter_add_batch+0x51/0x90 ? filemap_map_pages+0x515/0x660 __x64_sys_sendto+0x20/0x30 do_syscall_64+0x7b/0x2c0 ? do_read_fault+0x108/0x220 ? do_pte_missing+0x14a/0x3e0 ? __handle_mm_fault+0x321/0x730 ? count_memcg_events+0x13f/0x180 ? handle_mm_fault+0x1fb/0x2d0 ? do_user_addr_fault+0x20c/0x700 ? syscall_exit_work+0x104/0x140 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f0c25b0feca [...] ---[end trace 0000000000000000]---	N/A	More Details

CVE-2025-38627	In the Linux kernel, the following vulnerability has been resolved: f2fs: compress: fix UAF of f2fs_inode_info in f2fs_free_dic The decompress_io_ctx may be released asynchronously after I/O completion. If this file is deleted immediately after read, and the kworker of processing post_read_wq has not been executed yet due to high workloads, It is possible that the inode(f2fs_inode_info) is evicted and freed before it is used f2fs_free_dic. The UAF case as below: Thread A Thread B - f2fs_decompress_end_io - f2fs_put_dic - queue_work add free_dic work to post_read_wq - do_unlink - iput - evict - call_rcu This file is deleted after read. Thread C kworker to process post_read_wq - rcu_do_batch - f2fs_free_inode - kmem_cache_free inode is freed by rcu - process_scheduled_works - f2fs_late_free_dic - f2fs_free_dic - f2fs_release_decomp_mem read (dic->inode)->i_compress_algorithm This patch store compress_algorithm and sbi in dic to avoid inode UAF. In addition, the previous solution is deprecated in [1] may cause system hang. [1] https://lore.kernel.org/all/c36ab955-c8db-4a8b-a9d0-f07b5f426c3f@kernel.org	N/A	More Details
CVE-2025-38626	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to trigger foreground gc during f2fs_map_blocks() in lfs mode w/ "mode=lfs" mount option, generic/299 will cause system panic as below: ------------[cut here]------------ kernel BUG at fs/f2fs/segment.c:2835! Call Trace: <TASK> f2fs_allocate_data_block+0x6f4/0xc50 f2fs_map_blocks+0x970/0x1550 f2fs_iomap_begin+0xb2/0x1e0 iomap_iter+0x1d6/0x430 __iomap_dio_rw+0x208/0x9a0 f2fs_file_write_iter+0x6b3/0xfa0 aio_write+0x15d/0x2e0 io_submit_one+0x55e/0xab0 __x64_sys_io_submit+0xa5/0x230 do_syscall_64+0x84/0x2f0 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0010:new_curseg+0x70f/0x720 The root cause of we run out-of-space is: in f2fs_map_blocks(), f2fs may trigger foreground gc only if it allocates any physical block, it will be a little bit later when there is multiple threads writing data w/ aio/dio/bufio method in parallel, since we always use OPU in lfs mode, so f2fs_map_blocks() does block allocations aggressively. In order to fix this issue, let's give a chance to trigger foreground gc in prior to block allocation in f2fs_map_blocks().	N/A	More Details
CVE-2025-38625	In the Linux kernel, the following vulnerability has been resolved: vfio/pds: Fix missing detach_ioas op When CONFIG_IOMMUFD is enabled and a device is bound to the pds_vfio_pci driver, the following WARN_ON() trace is seen and probe fails: WARNING: CPU: 0 PID: 5040 at drivers/vfio/vfio_main.c:317 __vfio_register_dev+0x130/0x140 [vfio] <...> pds_vfio_pci 0000:08:00.1: probe with driver pds_vfio_pci failed with error -22 This is because the driver's vfio_device_ops.detach_ioas isn't set. Fix this by using the generic vfio_iommufd_physical_detach_ioas function.	N/A	More Details
CVE-2025-38643	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: Add missing lock in cfg80211_check_and_end_cac() Callers of wdev_chandef() must hold the wiphy mutex. But the worker cfg80211_propagate_cac_done_wk() never takes the lock. Which triggers the warning below with the mesh_peer_connected_dfs test from hostapd and not (yet) released mac80211 code changes: WARNING: CPU: 0 PID: 495 at net/wireless/chan.c:1552 wdev_chandef+0x60/0x165 Modules linked in: CPU: 0 UID: 0 PID: 495 Comm: kworker/u4:2 Not tainted 6.14.0-rc5-wt-g03960e6f9d47 #33 13c287eeabfe1efea01c0bcc863723ab082e17cf Workqueue: cfg80211 cfg80211_propagate_cac_done_wk Stack: 00000000 00000001 ffffff00 6093267c 00000000 6002ec30 6d577c50 60037608 00000000 67e8d108 6063717b 00000000 Call Trace: [<6002ec30>] ? _printk+0x0/0x98 [<6003c2b3>] show_stack+0x10e/0x11a [<6002ec30>] ? _printk+0x0/0x98 [<60037608>] dump_stack_lvl+0x71/0xb8 [<6063717b>] ? wdev_chandef+0x60/0x165 [<6003766d>] dump_stack+0x1e/0x20 [<6005d1b7>] __warn+0x101/0x20f [<6005d3a8>] warn_slowpath_fmt+0xe3/0x15d [<600b0c5c>] ? mark_lock.part.0+0x0/0x4ec [<60751191>] ? __this_cpu_preempt_check+0x0/0x16 [<600b11a2>] ? mark_held_locks+0x5a/0x6e [<6005d2c5>] ? warn_slowpath_fmt+0x0/0x15d [<60052e53>] ? unblock_signals+0x3a/0xe7 [<60052f2d>] ? um_set_signals+0x2d/0x43 [<60751191>] ? __this_cpu_preempt_check+0x0/0x16 [<607508b2>] ? lock_is_held_type+0x207/0x21f [<6063717b>] wdev_chandef+0x60/0x165 [<605f89b4>] regulatory_propagate_dfs_state+0x247/0x43f [<60052f00>] ? um_set_signals+0x0/0x43 [<605e6bfd>] cfg80211_propagate_cac_done_wk+0x3a/0x4a [<6007e460>] process_scheduled_works+0x3bc/0x60e [<6007d0ec>] ? move_linked_works+0x4d/0x81 [<6007d120>] ? assign_work+0x0/0xaa [<6007f81f>] worker_thread+0x220/0x2dc [<600786ef>] ? set_pf_worker+0x0/0x57 [<60087c96>] ? to_kthread+0x0/0x43 [<6008ab3c>] kthread+0x2d3/0x2e2 [<6007f5ff>] ? worker_thread+0x0/0x2dc [<6006c05b>] ? calculate_sigpending+0x0/0x56 [<6003b37d>] new_thread_handler+0x4a/0x64 irq event stamp: 614611 hardirqs last enabled at (614621): [<00000000600bc96b>] __up_console_sem+0x82/0xaf hardirqs last disabled at (614630): [<00000000600bc92c>] __up_console_sem+0x43/0xaf softirqs last enabled at (614268): [<00000000606c55c6>] __ieee80211_wake_queue+0x933/0x985 softirqs last disabled at (614266): [<00000000606c52d6>] __ieee80211_wake_queue+0x643/0x985	N/A	More Details
CVE-2025-38645	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Check device memory pointer before usage Add a NULL check before accessing device memory to prevent a crash if dev->dm allocation in mlx5_init_once() fails.	N/A	More Details
CVE-2025-38664	In the Linux kernel, the following vulnerability has been resolved: ice: Fix a null pointer dereference in ice_copy_and_init_pkg() Add check for the return value of devm_kmemdup() to prevent potential null pointer dereference.	N/A	More Details
CVE-2025-38646	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: avoid NULL dereference when RX problematic packet on unsupported 6 GHz band With a quite rare chance, RX report might be problematic to make SW think a packet is received on 6 GHz band even if the chip does not support 6 GHz band actually. Since SW won't initialize stuffs for unsupported bands, NULL dereference will happen then in the sequence, rtw89_vif_rx_stats_iter() -> rtw89_core_cancel_6ghz_probe_tx(). So, add a check to avoid it. The following is a crash log for this case. BUG: kernel NULL pointer dereference, address: 0000000000000032 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 1 PID: 1907 Comm: irq/131-rtw89_p Tainted: G U 6.6.56-05896-g89f5fb0eb30b #1 (HASH:1400 4) Hardware name: Google Telith/Telith, BIOS Google_Telith.15217.747.0 11/12/2024 RIP: 0010:rtw89_vif_rx_stats_iter+0xd2/0x310 [rtw89_core] Code: 4c 89 7d c8 48 89 55 c0 49 8d 44 24 02 48 89 45 b8 45 31 ff eb 11 41 c6 45 3a 01 41 b7 01 4d 8b 6d 00 4d 39 f5 74 42 8b 43 10 <41> 33 45 32 0f b7 4b 14 66 41 33 4d 36 0f b7 c9 09 c1 74 d8 4d 85 RSP: 0018:ffff9f3080138ca0 EFLAGS: 00010246 RAX: 00000000b8bf5770 RBX: ffff91b5e8c639c0 RCX: 0000000000000011 RDX: ffff91b582de1be8 RSI: 0000000000000000 RDI: ffff91b5e8c639e6 RBP: ffff9f3080138d00 R08: 0000000000000000 R09: 0000000000000000 R10: ffff91b59de70000 R11: ffffffffc069be50 R12: ffff91b5e8c639e4 R13: 0000000000000000 R14: ffff91b5828020b8 R15: 0000000000000000 FS: 0000000000000000(0000) GS:ffff91b8efa40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000032 CR3: 00000002bf838000 CR4: 0000000000750ee0 PKRU: 55555554 Call Trace: <IRQ> ? __die_body+0x68/0xb0 ? page_fault_oops+0x379/0x3e0 ? exc_page_fault+0x4f/0xa0 ? asm_exc_page_fault+0x22/0x30 ? __pfx_rtw89_vif_rx_stats_iter+0x10/0x10 [rtw89_core (HASH:1400 5)] ? rtw89_vif_rx_stats_iter+0xd2/0x310 [rtw89_core (HASH:1400 5)] __iterate_interfaces+0x59/0x110 [mac80211 (HASH:1400 6)] ? __pfx_rtw89_vif_rx_stats_iter+0x10/0x10 [rtw89_core (HASH:1400 5)] ? __pfx_rtw89_vif_rx_stats_iter+0x10/0x10 [rtw89_core (HASH:1400 5)] ieee80211_iterate_active_interfaces_atomic+0x36/0x50 [mac80211 (HASH:1400 6)] rtw89_core_rx_to_mac80211+0xfd/0x1b0 [rtw89_core (HASH:1400 5)] rtw89_core_rx+0x43a/0x980 [rtw89_core (HASH:1400 5)]	N/A	More Details
CVE-2025-38663	In the Linux kernel, the following vulnerability has been resolved: nilfs2: reject invalid file types when reading inodes To prevent inodes with invalid file types from tripping through the vfs and causing malfunctions or assertion failures, add a missing sanity check when reading an inode from a block device. If the file type is not valid, treat it as a filesystem error.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ASoC: mediatek: mt8365-dai-i2s: pass correct size to mt8365_dai_set_priv Given mt8365_dai_set_priv allocate priv_size space to copy priv_data which means we should pass mt8365_i2s_priv[i] or "struct mtk_afe_i2s_priv" instead of afe_priv which has the size of "struct mt8365_afe_private". Otherwise the		

CVE-2025-38662	KASAN complains about. [59.389765] BUG: KASAN: global-out-of-bounds in mt8365_dai_set_priv+0xc8/0x168 [snd_soc_mt8365_pcm] ... [59.394789] Call trace: [59.395167] dump_backtrace+0xa0/0x128 [59.395733] show_stack+0x20/0x38 [59.396238] dump_stack_lvl+0xe8/0x148 [59.396806] print_report+0x37c/0x5e0 [59.397358] kasan_report+0xac/0xf8 [59.397885] kasan_check_range+0xe8/0x190 [59.398485] asan_memcpy+0x3c/0x98 [59.399022] mt8365_dai_set_priv+0xc8/0x168 [snd_soc_mt8365_pcm] [59.399928] mt8365_dai_i2s_register+0x1e8/0x2b0 [snd_soc_mt8365_pcm] [59.400893] mt8365_afe_pcm_dev_probe+0x4d0/0xdf0 [snd_soc_mt8365_pcm] [59.401873] platform_probe+0xcc/0x228 [59.402442] really_probe+0x340/0x9e8 [59.402992] driver_probe_device+0x16c/0x3f8 [59.403638] driver_probe_device+0x64/0x1d8 [59.404256] driver_attach+0x1dc/0x4c8 [59.404840] bus_for_each_dev+0x100/0x190 [59.405442] driver_attach+0x44/0x68 [59.405980] bus_add_driver+0x23c/0x500 [59.406550] driver_register+0xf8/0x3d0 [59.407122] platform_driver_register+0x68/0x98 [59.407810] mt8365_afe_pcm_driver_init+0x2c/0xff8 [snd_soc_mt8365_pcm]	N/A	More Details
CVE-2025-38661	In the Linux kernel, the following vulnerability has been resolved: platform/x86: alienware-wmi-wmax: Fix `dmi_system_id` array Add missing empty member to `awcc_dmi_table`.	N/A	More Details
CVE-2025-38660	In the Linux kernel, the following vulnerability has been resolved: [ceph] parse_longname(): strrchr() expects NUL-terminated string ... and parse_longname() is not guaranteed that. That's the reason why it uses kmemdup_nul() to build the argument for kstrtou64(); the problem is, kstrtou64() is not the only thing that need it. Just get a NUL-terminated copy of the entire thing and be done with that...	N/A	More Details
CVE-2025-38659	In the Linux kernel, the following vulnerability has been resolved: gfs2: No more self recovery When a node withdraws and it turns out that it is the only node that has the filesystem mounted, gfs2 currently tries to replay the local journal to bring the filesystem back into a consistent state. Not only is that a very bad idea, it has also never worked because gfs2_recover_func() will refuse to do anything during a withdraw. However, before even getting to this point, gfs2_recover_func() dereferences sdp->sd_jdesc->jd_inode. This was a use-after-free before commit 04133b607a78 ("gfs2: Prevent double iput for journal on error") and is a NULL pointer dereference since then. Simply get rid of self recovery to fix that.	N/A	More Details
CVE-2025-38658	In the Linux kernel, the following vulnerability has been resolved: nvmet: pci-epf: Do not complete commands twice if nvmet_req_init() fails Have nvmet_req_init() and req->execute() complete failed commands. Description of the problem: nvmet_req_init() calls __nvmet_req_complete() internally upon failure, e.g., unsupported opcode, which calls the "queue_response" callback, this results in nvmet_pci_epf_queue_response() being called, which will call nvmet_pci_epf_complete_iod() if data_len is 0 or if dma_dir is different from DMA_TO_DEVICE. This results in a double completion as nvmet_pci_epf_exec_iod_work() also calls nvmet_pci_epf_complete_iod() when nvmet_req_init() fails. Steps to reproduce: On the host send a command with an unsupported opcode with nvme-cli, For example the admin command "security receive" $ sudo nvme security-recv /dev/nvme0n1 -n1 -x4096 This triggers a double completion as nvmet_req_init() fails and nvmet_pci_epf_queue_response() is called, here iod->dma_dir is still in the default state of "DMA_NONE" as set by default in nvmet_pci_epf_alloc_iod(), so nvmet_pci_epf_complete_iod() is called. Because nvmet_req_init() failed nvmet_pci_epf_complete_iod() is also called in nvmet_pci_epf_exec_iod_work() leading to a double completion. This not only sends two completions to the host but also corrupts the state of the PCI NVMe target leading to kernel oops. This patch lets nvmet_req_init() and req->execute() complete all failed commands, and removes the double completion case in nvmet_pci_epf_exec_iod_work() therefore fixing the edge cases where double completions occurred.	N/A	More Details
CVE-2025-38657	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: mcc: prevent shift wrapping in rtw89_core_mlsr_switch() The "link_id" value comes from the user via debugfs. If it's larger than BITS_PER_LONG then that would result in shift wrapping and potentially an out of bounds access later. In fact, we can limit it to IEEE80211_MLD_MAX_NUM_LINKS (15). Fortunately, only root can write to debugfs files so the security impact is minimal.	N/A	More Details
CVE-2025-38656	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: Fix error code in iwl_op_mode_dvm_start() Preserve the error code if iwl_setup_deferred_work() fails. The current code returns ERR_PTR(0) (which is NULL) on this path. I believe the missing error code potentially leads to a use after free involving debugfs.	N/A	More Details
CVE-2025-38655	In the Linux kernel, the following vulnerability has been resolved: pinctrl: canaan: k230: add NULL check in DT parse Add a NULL check for the return value of of_get_property() when retrieving the "pinmux" property in the group parser. This avoids a potential NULL pointer dereference if the property is missing from the device tree node. Also fix a typo ("sintenel") in the device ID match table comment, correcting it to "sentinel".	N/A	More Details
CVE-2025-38654	In the Linux kernel, the following vulnerability has been resolved: pinctrl: canaan: k230: Fix order of DT parse and pinctrl register Move DT parse before pinctrl register. This ensures that device tree parsing is done before calling devm_pinctrl_register() to prevent using uninitialized pin resources.	N/A	More Details
CVE-2025-38653	In the Linux kernel, the following vulnerability has been resolved: proc: use the same treatment to check proc_lseek as ones for proc_read_iter et.al Check pde->proc_ops->proc_lseek directly may cause UAF in rmmod scenario. It's a gap in proc_reg_open() after commit 654b33ada4ab("proc: fix UAF in proc_get_inode()"). Followed by Al Viro's suggestion, fix it in same manner.	N/A	More Details
CVE-2025-38652	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid out-of-boundary access in devs.path - touch /mnt/f2fs/0123456789012345678901234567890123456789012345678901234567890123 - truncate -s $((1024*1024*1024)) \ /mnt/f2fs/0123456789012345678901234567890123456789012345678901234567890123 - touch /mnt/f2fs/file - truncate -s $((1024*1024*1024)) /mnt/f2fs/file - mkfs.f2fs /mnt/f2fs/0123456789012345678901234567890123456789012345678901234567890123 \ -c /mnt/f2fs/file - mount /mnt/f2fs/0123456789012345678901234567890123456789012345678901234567890123 \ /mnt/f2fs/loop [16937.192225] F2FS-fs (loop0): Mount Device [0]: /mnt/f2fs/0123456789012345678901234567890123456789012345678901234567890123\xff\x01, 511, 0 - 3ffff [16937.192268] F2FS-fs (loop0): Failed to find devices If device path length equals to MAX_PATH_LEN, sbi->devs.path[] may not end up w/ null character due to path array is fully filled, So accidently, fields locate after path[] may be treated as part of device path, result in parsing wrong device path. struct f2fs_dev_info { ... char path[MAX_PATH_LEN]; ... }; Let's add one byte space for sbi->devs.path[] to store null character of device path string.	N/A	More Details
CVE-2025-38651	In the Linux kernel, the following vulnerability has been resolved: landlock: Fix warning from KUnit tests get_id_range() expects a positive value as first argument but get_random_u8() can return 0. Fix this by clamping it. Validated by running the test in a for loop for 1000 times. Note that MAX() is wrong as it is only supposed to be used for constants, but max() is good here. [..] ok 9 test_range2_rand1 [..] ok 10 test_range2_rand2 [..] ok 11 test_range2_rand15 [..] ------------[cut here]------------ [..] WARNING: CPU: 6 PID: 104 at security/landlock/id.c:99 test_range2_rand16 (security/landlock/id.c:99 (discriminator 1) security/landlock/id.c:234 (discriminator 1)) [..] Modules linked in: [..] CPU: 6 UID: 0 PID: 104 Comm: kunit_try_catch Tainted: G N 6.16.0-rc1-dev-00001-g314a2f98b65f #1 PREEMPT(undef) [..] Tainted: [N]=TEST [..] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [..] RIP: 0010:test_range2_rand16 (security/landlock/id.c:99 (discriminator 1) security/landlock/id.c:234 (discriminator 1)) [..] Code: 49 c7 c0 10 70 30 82 4c 89 ff 48 c7 c6 a0 63 1e 83 49 c7 45 a0 e0 63 1e 83 e8 3f 95 17 00 e9 1f ff ff ff 0f 0b e9 df fd ff ff <0f> 0b ba 01 00 00 00 e9 68 fe ff ff 49 89 45 a8 49 8d 4d a0 45 31 [..] RSP: 0000:ffff888104eb7c78 EFLAGS: 00010246 [..] RAX: 0000000000000000 RBX: 000000000870822c RCX: 0000000000000000 ^^^^^^^^^^^^^^^^^^ [..] [..] Call Trace: [..] [..] ---[end trace 0000000000000000]--- [..] ok 12 test_range2_rand16 [..] # landlock_id: pass:12 fail:0 skip:0 total:12 [..] # Totals: pass:12 fail:0	N/A	More Details

	skip:0 total:12 [..] ok 1 landlock_id [mic: Minor cosmetic improvements]		
CVE-2025-38650	In the Linux kernel, the following vulnerability has been resolved: hfsplus: remove mutex_lock check in hfsplus_free_extents Syzbot reported an issue in hfsplus filesystem: ------------[cut here]------------ WARNING: CPU: 0 PID: 4400 at fs/hfsplus/extents.c:346 hfsplus_free_extents+0x700/0xad0 Call Trace: <TASK> hfsplus_file_truncate+0x768/0xbb0 fs/hfsplus/extents.c:606 hfsplus_write_begin+0xc2/0xd0 fs/hfsplus/inode.c:56 cont_expand_zero fs/buffer.c:2383 [inline] cont_write_begin+0x2cf/0x860 fs/buffer.c:2446 hfsplus_write_begin+0x86/0xd0 fs/hfsplus/inode.c:52 generic_cont_expand_simple+0x151/0x250 fs/buffer.c:2347 hfsplus_setattr+0x168/0x280 fs/hfsplus/inode.c:263 notify_change+0xe38/0x10f0 fs/attr.c:420 do_truncate+0x1fb/0x2e0 fs/open.c:65 do_sys_ftruncate+0x2eb/0x380 fs/open.c:193 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd To avoid deadlock, Commit 31651c607151 ("hfsplus: avoid deadlock on file truncation") unlock extree before hfsplus_free_extents(), and add check wheather extree is locked in hfsplus_free_extents(). However, when operations such as hfsplus_file_release, hfsplus_setattr, hfsplus_unlink, and hfsplus_get_block are executed concurrently in different files, it is very likely to trigger the WARN_ON, which will lead syzbot and xfstest to consider it as an abnormality. The comment above this warning also describes one of the easy triggering situations, which can easily trigger and cause xfstest&syzbot to report errors. [task A] [task B] ->hfsplus_file_release ->hfsplus_file_truncate ->hfs_find_init ->mutex_lock ->mutex_unlock ->hfsplus_write_begin ->hfsplus_get_block ->hfsplus_file_extend ->hfsplus_ext_read_extent ->hfs_find_init ->mutex_lock ->hfsplus_free_extents WARN_ON(mutex_is_locked) !!! Several threads could try to lock the shared extents tree. And warning can be triggered in one thread when another thread has locked the tree. This is the wrong behavior of the code and we need to remove the warning.	N/A	More Details
CVE-2025-38649	In the Linux kernel, the following vulnerability has been resolved: arm64: dts: qcom: qcs615: fix a crash issue caused by infinite loop for Coresight An infinite loop has been created by the Coresight devices. When only a source device is enabled, the coresight_find_activated_sysfs_sink function is recursively invoked in an attempt to locate an active sink device, ultimately leading to a stack overflow and system crash. Therefore, disable the replicator1 to break the infinite loop and prevent a potential stack overflow. replicator1_out -> funnel_swao_in6 -> tmc_etf_swao_in -> tmc_etf_swao_out | | replicator1_in replicator_swao_in | | replicator0_out1 replicator_swao_out0 | | replicator0_in funnel_in1_in3 | | tmc_etf_out <- tmc_etf_in <- funnel_merg_out <- funnel_merg_in1 <- funnel_in1_out [call trace] dump_backtrace+0x9c/0x128 show_stack+0x20/0x38 dump_stack_lvl+0x48/0x60 dump_stack+0x18/0x28 panic+0x340/0x3b0 nmi_panic+0x94/0xa0 panic_bad_stack+0x114/0x138 handle_bad_stack+0x34/0xb8 __bad_stack+0x78/0x80 coresight_find_activated_sysfs_sink+0x28/0xa0 [coresight] coresight_find_activated_sysfs_sink+0x5c/0xa0 [coresight] coresight_find_activated_sysfs_sink+0x5c/0xa0 [coresight] coresight_find_activated_sysfs_sink+0x5c/0xa0 [coresight] coresight_find_activated_sysfs_sink+0x5c/0xa0 [coresight] ... coresight_find_activated_sysfs_sink+0x5c/0xa0 [coresight] coresight_enable_sysfs+0x80/0x2a0 [coresight] side effect after the change: Only trace data originating from AOSS can reach the ETF_SWAO and EUD sinks.	N/A	More Details
CVE-2025-38648	In the Linux kernel, the following vulnerability has been resolved: spi: stm32: Check for cfg availability in stm32_spi_probe The stm32_spi_probe function now includes a check to ensure that the pointer returned by of_device_get_match_data is not NULL before accessing its members. This resolves a warning where a potential NULL pointer dereference could occur when accessing cfg->has_device_mode. Before accessing the 'has_device_mode' member, we verify that 'cfg' is not NULL. If 'cfg' is NULL, an error message is logged. This change ensures that the driver does not attempt to access configuration data if it is not available, thus preventing a potential system crash due to a NULL pointer dereference.	N/A	More Details
CVE-2025-38647	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: sar: drop lockdep assertion in rtw89_set_sar_from_acpi The following assertion is triggered on the rtw89 driver startup. It looks meaningless to hold wiphy lock on the early init stage so drop the assertion. WARNING: CPU: 7 PID: 629 at drivers/net/wireless/realtek/rtw89/sar.c:502 rtw89_set_sar_from_acpi+0x365/0x4d0 [rtw89_core] CPU: 7 UID: 0 PID: 629 Comm: (udev-worker) Not tainted 6.15.0+ #29 PREEMPT(lazy) Hardware name: LENOVO 21D0/LNVNB161216, BIOS J6CN50WW 09/27/2024 RIP: 0010:rtw89_set_sar_from_acpi+0x365/0x4d0 [rtw89_core] Call Trace: <TASK> rtw89_sar_init+0x68/0x2c0 [rtw89_core] rtw89_core_init+0x188e/0x1e50 [rtw89_core] rtw89_pci_probe+0x530/0xb50 [rtw89_pci] local_pci_probe+0xd9/0x190 pci_call_probe+0x183/0x540 pci_device_probe+0x171/0x2c0 really_probe+0x1e1/0x890 __driver_probe_device+0x18c/0x390 driver_probe_device+0x4a/0x120 __driver_attach+0x1a0/0x530 bus_for_each_dev+0x10b/0x190 bus_add_driver+0x2eb/0x540 driver_register+0x1a3/0x3a0 do_one_initcall+0xd5/0x450 do_init_module+0x2cc/0x8f0 init_module_from_file+0xe1/0x150 idempotent_init_module+0x226/0x760 __x64_sys_finit_module+0xcd/0x150 do_syscall_64+0x94/0x380 entry_SYSCALL_64_after_hwframe+0x76/0x7e Found by Linux Verification Center (linuxtesting.org).	N/A	More Details
CVE-2025-43762	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.1, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allow users to upload an unlimited amount of files through the forms, the files are stored in the document_library allowing an attacker to cause a potential DDoS.	N/A	More Details
CVE-2025-8612	AOMEI Backupper Workstation Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of AOMEI Backupper Workstation. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. User interaction on the part of an administrator is needed additionally. The specific flaw exists within the restore functionality. By creating a junction, an attacker can abuse the service to create arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27059.	N/A	More Details
CVE-2025-57801	gnark is a zero-knowledge proof system framework. In versions prior to 0.14.0, the Verify function in eddsa.go and ecdsa.go used the S value from a signature without asserting that 0 ≤ S < order, leading to a signature malleability vulnerability. Because gnark's native EdDSA and ECDSA circuits lack essential constraints, multiple distinct witnesses can satisfy the same public inputs. In protocols where nullifiers or anti-replay checks are derived from R and S, this enables signature malleability and may allow double spending. This issue has been addressed in version 0.14.0.	N/A	More Details
CVE-2025-38624	In the Linux kernel, the following vulnerability has been resolved: PCI: pnv_php: Clean up allocated IRQs on unplug When the root of a nested PCIe bridge configuration is unplugged, the pnv_php driver leaked the allocated IRQ resources for the child bridges' hotplug event notifications, resulting in a panic. Fix this by walking all child buses and deallocating all its IRQ resources before calling pci_hp_remove_devices(). Also modify the lifetime of the workqueue at struct pnv_php_slot::wq so that it is only destroyed in pnv_php_free_slot(), instead of pnv_php_disable_irq(). This is required since pnv_php_disable_irq() will now be called by workers triggered by hot unplug interrupts, so the workqueue needs to stay allocated. The abridged kernel panic that occurs without this patch is as follows: WARNING: CPU: 0 PID: 687 at kernel/irq/msi.c:292 msi_device_data_release+0x6c/0x9c CPU: 0 UID: 0 PID: 687 Comm: bash Not tainted 6.14.0-rc5+ #2 Call Trace: msi_device_data_release+0x34/0x9c (unreliable) release_nodes+0x64/0x13c devres_release_all+0xc0/0x140 device_del+0x2d4/0x46c pci_destroy_dev+0x5c/0x194 pci_hp_remove_devices+0x90/0x128 pci_hp_remove_devices+0x44/0x128 pnv_php_disable_slot+0x54/0xd4 power_write_file+0xf8/0x18c pci_slot_attr_store+0x40/0x5c sysfs_kf_write+0x64/0x78 kernfs_fop_write_iter+0x1b0/0x290 vfs_write+0x3bc/0x50c ksys_write+0x84/0x140 system_call_exception+0x124/0x230 system_call_vectored_common+0x15c/0x2ec [bhelgaas: tidy comments]	N/A	More Details
CVE-2010-20123	Steinberg MyMP3Player version 3.0 (build 3.0.0.67) is vulnerable to a stack-based buffer overflow when parsing .m3u playlist files. The application fails to properly validate the length of input data within the playlist, allowing a specially crafted file to overwrite critical memory structures and execute arbitrary code. This vulnerability can be exploited locally by convincing a user to open a malicious .m3u	N/A	More Details

	file.		
CVE-2011-10024	MJM Core Player (likely now referred to as MJM Player) 2011 is vulnerable to a stack-based buffer overflow when parsing specially crafted .s3m music files. The vulnerability arises from improper bounds checking in the file parser, allowing an attacker to overwrite memory on the stack and execute arbitrary code. Exploitation is triggered when a user opens a malicious .s3m file, and the exploit bypasses DEP and ASLR protections using a ROP chain.	N/A	More Details
CVE-2011-10025	Subtitle Processor 7.7.1 contains a buffer overflow vulnerability in its .m3u file parser. When a crafted playlist file is opened, the application converts input to Unicode and copies it to a fixed-size stack buffer without proper bounds checking. This allows an attacker to overwrite the Structured Exception Handler (SEH) and execute arbitrary code.	N/A	More Details
CVE-2025-7426	Information disclosure and exposure of authentication FTP credentials over the debug port 1604 in the MINOVA TTA service. This allows unauthenticated remote access to an active FTP account containing sensitive internal data and import structures. In environments where this FTP server is part of automated business processes (e.g. EDI or data integration), this could lead to data manipulation, extraction, or abuse. Debug ports 1602, 1603 and 1636 also expose service architecture information and system activity logs	N/A	More Details
CVE-2025-5191	An Unquoted Search Path vulnerability has been identified in the utility for Moxa’s industrial computers (Windows). Due to the unquoted path configuration in the SerialInterfaceService.exe utility, a local attacker with limited privileges could place a malicious executable in a higher-priority directory within the search path. When the Serial Interface service starts, the malicious executable could be run with SYSTEM privileges. Successful exploitation could allow privilege escalation or enable an attacker to maintain persistence on the affected system. While successful exploitation can severely impact the confidentiality, integrity, and availability of the affected device itself, there is no loss of confidentiality, integrity, or availability within any subsequent systems.	N/A	More Details
CVE-2025-9118	A path traversal vulnerability in the NPM package installation process of Google Cloud Dataform allows a remote attacker to read and write files in other customers' repositories via a maliciously crafted package.json file.	N/A	More Details
CVE-2025-8997	An Information Exposure vulnerability has been identified in OpenText Enterprise Security Manager. The vulnerability could be remotely exploited.	N/A	More Details
CVE-2025-54301	A stored XSS vulnerability in Quantum Manager component 1.0.0-3.2.0 for Joomla was discovered. File names are not properly escaped.	N/A	More Details
CVE-2025-54300	A stored XSS vulnerability in Quantum Manager component 1.0.0-3.2.0 for Joomla was discovered. The SVG upload feature does not sanitize uploads.	N/A	More Details
CVE-2025-43747	A server-side request forgery (SSRF) vulnerability exists in the Liferay DXP 2025.Q2.0 through 2025.Q2.3 due to insecure domain validation on analytics.cloud.domain.allowed, allowing an attacker to perform requests by change the domain and bypassing the validation method, this insecure validation is not distinguishing between trusted subdomains and malicious domains.	N/A	More Details
CVE-2023-3948	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-4131	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-4143	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-43753	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.32 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.7, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 update 32 through update 92 allows an remote authenticated user to inject JavaScript into the embedded message field from the form container.	N/A	More Details
CVE-2025-43752	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15 and 7.4 GA through update 92 allow users to upload an unlimited amount of files through the object entries attachment fields, the files are stored in the document_library allowing an attacker to cause a potential DDoS.	N/A	More Details
CVE-2025-41451	Improper neutralization of alarm-to-mail configuration fields used in an OS shell Command ('Command Injection') in Danfoss AK-SM8xxA Series prior to version 4.3.1, leading to a potential post-authenticated remote code execution on an attacked system.	N/A	More Details
CVE-2025-41452	Post-authenticated external control of system web interface configuration setting vulnerability in Danfoss AK-SM8xxA Series prior to 4.3.1, which could allow for a denial of service attack induced by improper handling of exceptional conditions	N/A	More Details
CVE-2011-10023	MJM QuickPlayer (likely now referred to as MJM Player) version 2010 contains a stack-based buffer overflow vulnerability triggered by opening a malicious .s3m music file. The flaw occurs due to improper bounds checking in the file parser, allowing an attacker to overwrite memory and execute arbitrary code. Exploitation is achieved via a crafted payload that bypasses DEP and ASLR protections using ROP techniques, and requires user interaction to open the file.	N/A	More Details
CVE-2011-10021	Magix Musik Maker 16 is vulnerable to a stack-based buffer overflow due to improper handling of .mmm arrangement files. The vulnerability arises from an unsafe strcpy() operation that fails to validate input length, allowing attackers to overwrite the Structured Exception Handler (SEH). By crafting a malicious .mmm file, an attacker can trigger the overflow when the file is opened, potentially leading to arbitrary code execution. This vulnerability was remediated in version 17.	N/A	More Details
CVE-2011-10027	AOL Desktop 9.6 contains a buffer overflow vulnerability in its Tool\rich.rct component when parsing .rtx files. By embedding an overly long string in a hyperlink tag, an attacker can trigger a stack-based buffer overflow due to the use of unsafe strcpy operations. This allows remote attackers to execute arbitrary code when a victim opens a malicious .rtx file. AOL Desktop is end-of-life and no longer supported. Users are encouraged to migrate to AOL Desktop Gold or alternative platforms.	N/A	More Details

CVE-2011-10020	Kaillera Server version 0.86 is vulnerable to a denial-of-service condition triggered by sending a malformed UDP packet after the initial handshake. Once a client sends a valid HELLO0.83 packet and receives a response, any subsequent malformed packet causes the server to crash and become unresponsive. This flaw stems from improper input validation in the server's UDP packet handler, allowing unauthenticated remote attackers to disrupt service availability.	N/A	More Details
CVE-2025-8449	CWE-400: Uncontrolled Resource Consumption vulnerability exists that could cause a denial of service when an authenticated user sends a specially crafted request to a specific endpoint from within the BMS network.	N/A	More Details
CVE-2025-9074	A vulnerability was identified in Docker Desktop that allows local running Linux containers to access the Docker Engine API via the configured Docker subnet, at 192.168.65.7:2375 by default. This vulnerability occurs with or without Enhanced Container Isolation (ECI) enabled, and with or without the "Expose daemon on tcp://localhost:2375 without TLS" option enabled. This can lead to execution of a wide range of privileged commands to the engine API, including controlling other containers, creating new ones, managing images etc. In some circumstances (e.g. Docker Desktop for Windows with WSL backend) it also allows mounting the host drive with the same privileges as the user running Docker Desktop.	N/A	More Details
CVE-2010-20108	FTPPad <= 1.2.0 contains a stack-based buffer overflow vulnerability in its FTP directory listing parser. When the client connects to an FTP server and receives a crafted response to a LIST command containing an excessively long directory and filename, the application fails to properly validate input length. This results in a buffer overflow that overwrites the saved Extended Instruction Pointer (EIP), allowing remote attackers to execute arbitrary code.	N/A	More Details
CVE-2010-20113	EasyFTP Server 1.7.0.11 and earlier contains a stack-based buffer overflow vulnerability in its HTTP interface. When processing a GET request to list.html, the server fails to properly validate the length of the path parameter. Supplying an excessively long value causes a buffer overflow on the stack, potentially corrupting control flow structures. The vulnerability is exposed through the embedded web server and does not require authentication due to default anonymous access. The issue was resolved in version 1.7.0.12, after which the product was renamed to UplusFtp.	N/A	More Details
CVE-2025-43748	Insufficient CSRF protection for omni-administrator users in Liferay Portal 7.0.0 through 7.4.3.119, and Liferay DXP 2024.Q1.1 through 2024.Q1.6, 2023.Q4.0 through 2023.Q4.9, 2023.Q3.1 through 2023.Q3.9, 7.4 GA through update 92, 7.3 GA through update 36, and older unsupported versions allows attackers to execute Cross-Site Request Forgery	N/A	More Details
CVE-2009-10005	ContentKeeper Web Appliance (now maintained by Impero Software) versions prior to 125.10 expose the mimencode binary via a CGI endpoint, allowing unauthenticated attackers to retrieve arbitrary files from the filesystem. By crafting a POST request to /cgi-bin/ck/mimencode with traversal and output parameters, attackers can read sensitive files such as /etc/passwd outside the webroot.	N/A	More Details
CVE-2010-10014	Odin Secure FTP <= 4.1 is vulnerable to a stack-based buffer overflow when parsing directory listings received in response to an FTP LIST command. A malicious FTP server can send an overly long filename in the directory listing, which overflows a fixed-size stack buffer in the client and overwrites the Structured Exception Handler (SEH). This allows remote attackers to execute arbitrary code on the client system.	N/A	More Details
CVE-2010-20114	VariCAD EN up to and including version 2010-2.05 is vulnerable to a stack-based buffer overflow when parsing .dwb drawing files. The application fails to properly validate the length of input data embedded in the file, allowing a crafted .dwb file to overwrite critical memory structures. This flaw can be exploited locally by convincing a user to open a malicious file, resulting in arbitrary code execution.	N/A	More Details
CVE-2010-20042	Xion Audio Player versions prior to 1.0.126 are vulnerable to a Unicode-based stack buffer overflow triggered by opening a specially crafted .m3u playlist file. The file contains an overly long string that overwrites the Structured Exception Handler (SEH) chain, allowing an attacker to hijack execution flow and run arbitrary code.	N/A	More Details
CVE-2010-20045	FileWrangler <= 5.30 suffers from a stack-based buffer overflow vulnerability when parsing directory listings from an FTP server. A malicious server can send an overlong folder name in response to a LIST command, triggering memory corruption during client-side rendering. Exploitation requires passive user interaction—simply connecting to the server—without further input. Successful exploitation may lead to arbitrary code execution.	N/A	More Details
CVE-2010-20115	Arcane Software's Vermillion FTP Daemon (vftpd) versions up to and including 1.31 contains a memory corruption vulnerability triggered by a malformed FTP PORT command. The flaw arises from an out-of-bounds array access during input parsing, allowing an attacker to manipulate stack memory and potentially execute arbitrary code. Exploitation requires direct access to the FTP service and is constrained by a single execution attempt if the daemon is installed as a Windows service.	N/A	More Details
CVE-2010-20120	Maple versions up to and including 13's Maplet framework allows embedded commands to be executed automatically when a .maplet file is opened. This behavior bypasses standard security restrictions that normally prevent code execution in regular Maple worksheets. The vulnerability enables attackers to craft malicious .maplet files that execute arbitrary code without user interaction.	N/A	More Details
CVE-2010-20122	Xftp FTP Client version up to and including 3.0 (build 0238) contain a stack-based buffer overflow vulnerability triggered by a maliciously crafted PWD response from an FTP server. When the client connects to a server and receives an overly long directory string in response to the PWD command, the client fails to properly validate the length of the input before copying it into a fixed-size buffer. This results in memory corruption and allows remote attackers to execute arbitrary code on the client system.	N/A	More Details
CVE-2010-20049	LeapFTP < 3.1.x contains a stack-based buffer overflow vulnerability in its FTP client parser. When the client receives a directory listing containing a filename longer than 528 bytes, the application fails to properly bound-check the input and overwrites the Structured Exception Handler (SEH) chain. This allows an attacker operating a malicious FTP server to execute arbitrary code on the victim's machine when the file is listed or downloaded.	N/A	More Details
CVE-2025-54370	PhpOffice/PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. Prior to versions 1.30.0, 2.1.12, 2.4.0, 3.10.0, and 5.0.0, SSRF can occur when a processed HTML document is read and displayed in the browser. The vulnerability lies in the setPath method of the PhpOffice\PhpSpreadsheet\Worksheet\Drawing class, where a crafted string from the user is passed to the HTML reader. This issue has been patched in versions 1.30.0, 2.1.12, 2.4.0, 3.10.0, and 5.0.0.	N/A	More Details
CVE-2010-20059	FreeNAS 0.7.2 prior to revision 5543 includes an unauthenticated command-execution backdoor in its web interface. The exec_raw.php script exposes a cmd parameter that is passed directly to the underlying shell without sanitation.	N/A	More Details
CVE-2010-20103	A malicious backdoor was embedded in the official ProFTPD 1.3.3c source tarball distributed between November 28 and December 2, 2010. The backdoor implements a hidden FTP command trigger that, when invoked, causes the server to execute arbitrary shell commands with root privileges. This allows remote, unauthenticated attackers to run any OS command on the FTP server host.	N/A	More Details
CVE-2011-	Spreecommerce versions prior to 0.50.x contain a remote command execution vulnerability in the API's search functionality. Improper input sanitation allows attackers to inject arbitrary shell commands via the search[instance_eval] parameter, which is dynamically	N/A	More

10026	invoked using Ruby’s send method. This flaw enables unauthenticated attackers to execute commands on the server.		Details
CVE-2025-57699	Western Digital Kitfox for Windows provided by Western Digital Corporation registers a Windows service with an unquoted file path. A user with the write permission on the root directory of the system drive may execute arbitrary code with the SYSTEM privilege.	N/A	More Details
CVE-2025-8611	AOMEI Cyber Backup Missing Authentication for Critical Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of AOMEI Cyber Backup. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DaoService service, which listens on TCP port 9074 by default. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-26158.	N/A	More Details
CVE-2025-58037	Rejected reason: Not used	N/A	More Details
CVE-2025-58035	Rejected reason: Not used	N/A	More Details
CVE-2025-43769	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q3.1 through 2024.Q3.8, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows remote attackers to execute arbitrary web script or HTML via components tab.	N/A	More Details
CVE-2025-43768	Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15 and 7.4 GA through update 92 allows authenticated users without any permissions to access sensitive information of admin users using JSONWS APIs.	N/A	More Details
CVE-2025-24469	Rejected reason: Not used	N/A	More Details
CVE-2025-24468	Rejected reason: Not used	N/A	More Details
CVE-2025-22864	Rejected reason: Not used	N/A	More Details
CVE-2025-22863	Rejected reason: Not used	N/A	More Details
CVE-2025-22861	Rejected reason: Not used	N/A	More Details
CVE-2025-22860	Rejected reason: Not used	N/A	More Details
CVE-2025-43770	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.3, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the referer or FORWARD_URL using %00 in those parameters.	N/A	More Details
CVE-2025-8193	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-6181	The StrongDM Windows service incorrectly handled input validation. Authenticated attackers could potentially exploit this leading to privilege escalation.	N/A	More Details
CVE-2025-6182	The StrongDM Windows service incorrectly handled communication related to system certificate management. Attackers could exploit this behavior to install untrusted root certificates or remove trusted ones.	N/A	More Details
CVE-2025-6183	The StrongDM macOS client incorrectly processed JSON-formatted messages. Attackers could potentially modify macOS system configuration by crafting a malicious JSON message.	N/A	More Details
CVE-2025-52450	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Salesforce Tableau Server on Windows, Linux (abdoc api - create-data-source-from-file-upload modules) allows Absolute Path Traversal.This issue affects Tableau Server: before 2025.1.3, before 2024.2.12, before 2023.3.19.	N/A	More Details
CVE-2025-43761	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.4, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the frontend-editor-ckeditor-web/ckeditor/samples/old/ajax.html path	N/A	More Details
CVE-2025-8610	AOMEI Cyber Backup Missing Authentication for Critical Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of AOMEI Cyber Backup. Authentication is not required to exploit this vulnerability. The specific flaw exists within the StorageNode service, which listens on TCP port 9075 by default. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-26156.	N/A	More Details
CVE-			

2025-58036	Rejected reason: Not used	N/A	More Details
CVE-2025-58038	Rejected reason: Not used	N/A	More Details
CVE-2025-9341	Uncontrolled Resource Consumption vulnerability in Legion of the Bouncy Castle Inc. Bouncy Castle for Java FIPS bc-fips on All (API modules) allows Excessive Allocation. This vulnerability is associated with program files org/bouncycastle/crypto/fips/AESNativeCBC.Java. This issue affects Bouncy Castle for Java FIPS: from BC-FJA 2.1.0 through 2.1.0.	N/A	More Details
CVE-2025-58039	Rejected reason: Not used	N/A	More Details
CVE-2025-9340	Out-of-bounds Write vulnerability in Legion of the Bouncy Castle Inc. Bouncy Castle for Java bc-fips on All (API modules). This vulnerability is associated with program files org/bouncycastle/jcajce/provider/BaseCipher. This issue affects Bouncy Castle for Java: from BC-FJA 2.1.0 through 2.1.0.	N/A	More Details
CVE-2011-10028	The RealNetworks RealArcade platform includes an ActiveX control (InstallerDlg.dll, version 2.6.0.445) that exposes a method named Exec via the StubbyUtil.ProcessMgr COM object. This method allows remote attackers to execute arbitrary commands on a victim's Windows machine without proper validation or restrictions. This platform was sometimes referred to or otherwise known as RealArcade or Arcade Games and has since consolidated with RealNetworks' platform, GameHouse.	N/A	More Details
CVE-2011-10029	Solar FTP Server fails to properly handle format strings passed to the USER command. When a specially crafted string containing format specifiers is sent, the server crashes due to a read access violation in the __output_1() function of sfsservice.exe. This results in a denial of service (DoS) condition.	N/A	More Details
CVE-2011-10030	Foxit PDF Reader < 4.3.1.0218 exposes a JavaScript API function, createDataObject(), that allows untrusted PDF content to write arbitrary files anywhere on disk. By embedding a malicious PDF that calls this API, an attacker can drop executables or scripts into privileged folders, leading to code execution the next time the system boots or the user logs in.	N/A	More Details
CVE-2012-10061	Sockso Music Host Server versions <= 1.5 are vulnerable to a path traversal flaw that allows unauthenticated remote attackers to read arbitrary files from the server’s filesystem. The vulnerability exists in the HTTP interface on port 4444, where the endpoint /file/ fails to properly sanitize user-supplied input. Attackers can traverse directories and access sensitive files outside the intended web root.	N/A	More Details
CVE-2025-55751	OnboardLite is the result of the Influx Initiative, our vision for an improved student organization lifecycle at the University of Central Florida. An attacker can craft a link to the trusted application that, when visited, redirects the user to a malicious external site. This enables phishing, credential theft, malware delivery, and trust abuse. Any version with commit hash 6cca19e or later implements jwt signing for the redirect url parameter.	N/A	More Details
CVE-2010-20010	Foxit PDF Reader before 4.2.0.0928 does not properly bound-check the /Title entry in the PDF Info dictionary. A specially crafted PDF with an overlong Title string can overflow a fixed-size stack buffer, corrupt the Structured Exception Handler (SEH) chain, and lead to arbitrary code execution in the context of the user who opens the file.	N/A	More Details
CVE-2025-5352	A critical stored Cross-Site Scripting (XSS) vulnerability exists in the Analytics component of lunary-ai/lunary versions up to 1.9.23, where the NEXT_PUBLIC_CUSTOM_SCRIPT environment variable is directly injected into the DOM using dangerouslySetInnerHTML without any sanitization or validation. This allows arbitrary JavaScript execution in all users' browsers if an attacker can control the environment variable during deployment or through server compromise. The vulnerability can lead to complete account takeover, data exfiltration, malware distribution, and persistent attacks affecting all users until the environment variable is cleaned. The issue is fixed in version 1.9.25.	N/A	More Details
CVE-2025-6180	The StrongDM Client insufficiently protected a pre-authentication token. Attackers could exploit this to intercept and reuse the token, potentially redeeming valid authentication credentials through a race condition.	N/A	More Details
CVE-2025-43766	The Liferay Portal 7.4.0 through 7.3.3.131, and Liferay DXP 2024.Q4.0, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows the upload of unrestricted files in the style books component that are processed within the environment enabling arbitrary code execution by attackers.	N/A	More Details
CVE-2025-43765	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.13 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the text field from a web content.	N/A	More Details
CVE-2025-43764	Self-ReDoS (Regular expression Denial of Service) exists with Role Name search field of Kaleo Designer portlet JavaScript in Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.1, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.20 and 7.4 GA through update 92, which allows authenticated users with permissions to update Kaleo Workflows to enter a malicious Regex pattern causing their browser to hang for a very long time.	N/A	More Details
CVE-2025-43767	Open Redirect vulnerability in /c/portal/edit_info_item parameter redirect in Liferay Portal 7.4.3.86 through 7.4.3.131, and Liferay DXP 2024.Q3.1 through 2024.Q3.9, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 update 86 through update 92 allows an attacker to exploit this security vulnerability to redirect users to a malicious site.	N/A	More Details
CVE-2025-58043	Rejected reason: Not used	N/A	More Details
CVE-2025-58042	Rejected reason: Not used	N/A	More Details
CVE-2025-58041	Rejected reason: Not used	N/A	More Details
CVE-2025-	Rejected reason: Not used	N/A	More

58040			Details
CVE-2025-57755	claude-code-router is a powerful tool to route Claude Code requests to different models and customize any request. Due to improper Cross-Origin Resource Sharing (CORS) configuration, there is a risk that user API Keys or equivalent credentials may be exposed to untrusted domains. Attackers could exploit this misconfiguration to steal credentials, abuse accounts, exhaust quotas, or access sensitive data. The issue has been patched in v1.0.34.	N/A	More Details