SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 January 2026

Generated on 14 January 2026

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-2025-64093	Remote Code Execution vulnerability that allows unauthenticated attackers to inject arbitrary commands into the hostname of the device.	10.0	More Details
CVE-2025-70974	Fastjson before 1.2.48 mishandles autoType because, when an @type key is in a JSON document, and the value of that key is the name of a Java class, there may be calls to certain public methods of that class. Depending on the behavior of those methods, there may be JNDI injection with an attacker-supplied payload located elsewhere in that JSON document. This was exploited in the wild in 2023 through 2025. NOTE: this issue exists because of an incomplete fix for CVE-2017-18349. Also, a later bypass is covered by CVE-2022-25845.	10.0	More Details
CVE-2025-52694	Successful exploitation of the SQL injection vulnerability could allow an unauthenticated remote attacker to execute arbitrary SQL commands on the vulnerable service when it is exposed to the Internet.	10.0	More Details
CVE-2025-68271	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. From 5.0.0 to 6.10.1, OpenC3 COSMOS contains a critical remote code execution vulnerability reachable through the JSON-RPC API. When a JSON-RPC request uses the string form of certain APIs, attacker-controlled parameter text is parsed into values using String#convert_to_value. For array-like inputs, convert_to_value executes eval(). Because the cmd code path parses the command string before calling authorize(), an unauthenticated attacker can trigger Ruby code execution even though the request ultimately fails authorization (401). This vulnerability is fixed in 6.10.2.	10.0	More Details
CVE-2026-21858	n8n is an open source workflow automation platform. Versions starting with 1.65.0 and below 1.121.0 enable an attacker to access files on the underlying server through execution of certain form-based workflows. A vulnerable workflow could grant access to an unauthenticated remote attacker, resulting in exposure of sensitive information stored on the system and may enable further compromise depending on deployment configuration and workflow usage. This issue is fixed in version 1.121.0.	10.0	More Details
CVE-2025-63314	A static password reset token in the password reset function of DDSN Interactive Acora CMS v10.7.1 allows attackers to arbitrarily reset the user password and execute a full account takeover via a replay attack.	10.0	More Details
CVE-2025-64090	This vulnerability allows authenticated attackers to execute commands via the hostname of the device.	10.0	More Details
	XWiki Full Calendar Macro displays objects from the wiki on the calendar. Prior to version 2.4.5, users		

CVE-2025-65091	with the right to view the Calendar.JSONService page (including guest users) can exploit a SQL injection vulnerability by accessing database info or starting a DoS attack. This issue has been patched in version 2.4.5.	10.0	More Details
CVE-2025-61492	A command injection vulnerability in the execute_command function of terminal-controller-mcp 0.1.7 allows attackers to execute arbitrary commands via a crafted input.	10.0	More Details
CVE-2026-0881	Sandbox escape in the Messaging System component. This vulnerability affects Firefox < 147.	10.0	More Details
CVE-2025-40805	Affected devices do not properly enforce user authentication on specific API endpoints. This could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user. Successful exploitation requires that the attacker has learned the identity of a legitimate user.	10.0	More Details
CVE-2026-22688	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.5, there is a command injection vulnerability that allows authenticated users to inject stdio_config.command/args into MCP stdio settings, causing the server to execute subprocesses using these injected values. This issue has been patched in version 0.2.5.	9.9	More Details
CVE-2025-46066	An issue in Automai Director v.25.2.0 allows a remote attacker to escalate privileges	9.9	More Details
CVE-2026-21877	n8n is an open source workflow automation platform. In versions 0.121.2 and below, an authenticated attacker may be able to execute malicious code using the n8n service. This could result in full compromise and can impact both self-hosted and n8n Cloud instances. This issue is fixed in version 1.121.3. Administrators can reduce exposure by disabling the Git node and limiting access for untrusted users, but upgrading to the latest version is recommended.	9.9	More Details
CVE-2026-0501	Due to insufficient input validation in SAP S/4HANA Private Cloud and On-Premise (Financials General Ledger), an authenticated user could execute crafted SQL queries to read, modify, and delete backend database data. This leads to a high impact on the confidentiality, integrity, and availability of the application.	9.9	More Details
CVE-2025-46070	An issue in Automai BotManager v.25.2.0 allows a remote attacker to execute arbitrary code via the BotManager.exe component	9.8	More Details
CVE-2025-65552	D3D Wi-Fi Home Security System ZX-G12 v2.1.1 is vulnerable to RF replay attacks on the 433 MHz sensor communication channel. The system does not implement rolling codes, message authentication, or anti-replay protection, allowing an attacker within RF range to record valid alarm/control frames and replay them to trigger false alarms.	9.8	More Details
CVE-2025-66802	Sourcecodester Covid-19 Contact Tracing System 1.0 is vulnerable to RCE (Remote Code Execution). The application receives a reverse shell (php) into imagem of the user enabling RCE.	9.8	More Details
CVE-2025-67147	Multiple SQL Injection vulnerabilities exist in amansuryawanshi Gym-Management-System-PHP 1.0 via the 'name', 'email', and 'comment' parameters in (1) submit_contact.php, the 'username' and 'pass_key' parameters in (2) secure_login.php, and the 'login_id', 'pwfield', and 'login_key' parameters in (3) change_s_pwd.php. An unauthenticated or authenticated attacker can exploit these issues to bypass authentication, execute arbitrary SQL commands, modify database records, delete data, or escalate privileges to administrator level.	9.8	More Details
CVE-2025-15471	A vulnerability was detected in TRENDnet TEW-713RE 1.02. The impacted element is an unknown function of the file /goformX/formFSrvX. The manipulation of the argument SZCMD results in os command injection. It is possible to launch the attack 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.	9.8	More Details
CVE-2025-15501	A vulnerability was determined in Sangfor Operation and Maintenance Management System up to 3.0.8. Impacted is the function WriterHandle.getCmd of the file /isomp-protocol/protocol/getCmd. This manipulation of the argument sessionPath causes os command injection. Remote exploitation of the attack is possible. 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.	9.8	More Details
CVE-2025-29329	Buffer Overflow in the ippprint (Internet Printing Protocol) service in Sagemcom F@st 3686 MAGYAR_4.121.0 allows remote attacker to execute arbitrary code by sending a crafted HTTP request.	9.8	More Details
CVE-2025-15500	A vulnerability was found in Sangfor Operation and Maintenance Management System up to 3.0.8. This issue affects some unknown processing of the file /isomp-protocol/protocol/getHis of the component HTTP POST Request Handler. The manipulation of the argument sessionPath results in os command injection. The attack may be launched 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.	9.8	More Details
	EDIMAX BR-6208AC V2_1.02 is vulnerable to Command Injection. This arises because the pppUserName		

CVE-2025-70161	field is directly passed to a shell command via the system() function without proper sanitization. An attacker can exploit this by injecting malicious commands into the pppUserName field, allowing arbitrary code execution.	9.8	More Details
CVE-2025-69542	A Command Injection Vulnerability has been discovered in the DHCP daemon service of D-Link DIR895LA1 v102b07. The vulnerability exists in the lease renewal processing logic where the DHCP hostname parameter is directly concatenated into a system command without proper sanitization. When a DHCP client renews an existing lease with a malicious hostname, arbitrary commands can be executed with root privileges.	9.8	More Details
CVE-2025-14598	BeeS Software Solutions BET Portal contains an SQL injection vulnerability in the login functionality of affected sites. The vulnerability enables arbitrary SQL commands to be executed on the backend database.	9.8	More Details
CVE-2025-14736	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.28.25. This is due to insufficient validation of user-supplied role values in the 'validate_value', 'pre_update_value', and 'get_fields_display' functions. This makes it possible for unauthenticated attackers to register as administrators and gain complete control of the site, granted they can access a user registration form containing a Role field.	9.8	More Details
CVE-2025-15018	The Optional Email plugin for WordPress is vulnerable to Privilege Escalation via Account Takeover in all versions up to, and including, 1.3.11. This is due to the plugin not restricting its 'random_password' filter to registration contexts, allowing the filter to affect password reset key generation. This makes it possible for unauthenticated attackers to set a known password reset key when initiating a password reset, reset the password of any user including administrators, and gain access to their accounts.	9.8	More Details
CVE-2025-66913	JimuReport thru version 2.1.3 is vulnerable to remote code execution when processing user-controlled H2 JDBC URLs. The application passes the attacker-supplied JDBC URL directly to the H2 driver, allowing the use of certain directives to execute arbitrary Java code. A different vulnerability than CVE-2025-10770.	9.8	More Details
CVE-2025-67325	Unrestricted file upload in the hotel review feature in QloApps versions 1.7.0 and earlier allows remote unauthenticated attackers to achieve remote code execution.	9.8	More Details
CVE-2026-22584	Improper Control of Generation of Code ('Code Injection') vulnerability in Salesforce Uni2TS on MacOS, Windows, Linux allows Leverage Executable Code in Non-Executable Files.This issue affects Uni2TS: through 1.2.0.	9.8	More Details
CVE-2026-0879	Sandbox escape due to incorrect boundary conditions in the Graphics component. This vulnerability affects Firefox < 147, Firefox ESR < 115.32, and Firefox ESR < 140.7.	9.8	More Details
CVE-2025-10915	The Dreamer Blog WordPress theme through 1.2 is vulnerable to arbitrary installations due to a missing capability check.	9.8	More Details
CVE-2022-50919	Tdarr 2.00.15 contains an unauthenticated remote code execution vulnerability in its Help terminal that allows attackers to inject and chain arbitrary commands. Attackers can exploit the lack of input filtering by chaining commands like `--help; curl .py | python` to execute remote code without authentication.	9.8	More Details
CVE-2023-54335	eXtplorer 2.1.14 contains an authentication bypass vulnerability that allows attackers to login without a password by manipulating the login request. Attackers can exploit this flaw to upload malicious PHP files and execute remote commands on the vulnerable file management system.	9.8	More Details
CVE-2023-54334	Explorer32++ 1.3.5.531 contains a buffer overflow vulnerability in Structured Exception Handler (SEH) records that allows attackers to execute arbitrary code. Attackers can exploit the vulnerability by providing a long file name argument over 396 characters to corrupt the SEH chain and potentially execute malicious code.	9.8	More Details
CVE-2023-54330	Inbit Messenger versions 4.6.0 to 4.9.0 contain a remote stack-based buffer overflow vulnerability that allows unauthenticated attackers to execute arbitrary code by sending malformed network packets. Attackers can craft a specially designed payload targeting the messenger's network handler to overwrite the Structured Exception Handler (SEH) and execute shellcode on vulnerable Windows systems.	9.8	More Details
CVE-2023-54329	Inbit Messenger 4.6.0 - 4.9.0 contains a remote command execution vulnerability that allows unauthenticated attackers to execute arbitrary commands by exploiting a stack overflow in the messenger's protocol. Attackers can send specially crafted XML packets to port 10883 with a malicious payload to trigger the vulnerability and execute commands with system privileges.	9.8	More Details
CVE-2023-54328	AimOne Video Converter 2.04 Build 103 contains a buffer overflow vulnerability in its registration form that causes application crashes. Attackers can generate a 7000-byte payload to trigger the denial of service and potentially exploit the software's registration mechanism.	9.8	More Details
CVE-2022-	Flame II HSPA USB Modem contains an unquoted service path vulnerability in its Windows service configuration. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\Internet	9.8	More

50935	Telcel\ApplicationController.exe' to execute arbitrary code with elevated system privileges.		Details
CVE-2022-50926	WAGO 750-8212 PFC200 G2 2ETH RS firmware contains a privilege escalation vulnerability that allows attackers to manipulate user session cookies. Attackers can modify the cookie's 'name' and 'roles' parameters to elevate from ordinary user to administrative privileges without authentication.	9.8	More Details
CVE-2022-50925	Prowise Reflect version 1.0.9 contains a remote keystroke injection vulnerability that allows attackers to send keyboard events through an exposed WebSocket on port 8082. Attackers can craft malicious web pages to inject keystrokes, opening applications and typing arbitrary text by sending specific WebSocket messages.	9.8	More Details
CVE-2022-50922	Audio Conversion Wizard v2.01 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory with a specially crafted registration code. Attackers can generate a payload that overwrites the application's memory stack, potentially enabling remote code execution through a carefully constructed input buffer.	9.8	More Details
CVE-2022-50912	ImpressCMS 1.4.4 contains a file upload vulnerability with weak extension sanitization that allows attackers to upload potentially malicious files. Attackers can bypass file upload restrictions by using alternative file extensions .php2.php6.php7.phps.pht to execute arbitrary PHP code on the server.	9.8	More Details
CVE-2025-67825	An issue was discovered in Nitro PDF Pro for Windows before 14.42.0.34. In certain cases, it displays signer information from a non-verified PDF field rather than from the verified certificate subject. This could allow a document to present inconsistent signer details. The display logic was updated to ensure signer information consistently reflects the verified certificate identity.	9.8	More Details
CVE-2022-50905	e107 CMS version 3.2.1 contains multiple vulnerabilities that allow cross-site scripting (XSS) attacks. The first vulnerability is a reflected XSS that occurs in the news comment functionality when authenticated users interact with the comment form. An attacker can inject malicious JavaScript code through the URL parameter that gets executed when users click outside the comment field after typing content. The second vulnerability involves an upload restriction bypass for authenticated administrators, allowing them to upload SVG files containing malicious code through the media manager's remote URL upload feature. This results in stored XSS when the uploaded SVG files are accessed. These vulnerabilities were discovered by Hubert Wojciechowski and affect the news.php and image.php components of the CMS.	9.8	More Details
CVE-2022-50894	VIAVIWEB Wallpaper Admin 1.0 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the img_id parameter. Attackers can send GET requests to edit_gallery_image.php with malicious img_id values to extract database information.	9.8	More Details
CVE-2022-50893	VIAVIWEB Wallpaper Admin 1.0 contains an unauthenticated remote code execution vulnerability in the image upload functionality. Attackers can upload a malicious PHP file through the add_gallery_image.php endpoint to execute arbitrary code on the server.	9.8	More Details
CVE-2022-50807	Concrete5 CMS version 9.1.3 contains an XPath injection vulnerability that allows attackers to manipulate URL path parameters with malicious payloads. Attackers can flood the system with crafted requests to potentially extract internal content paths and system information.	9.8	More Details
CVE-2020-36911	Covenant 0.1.3 - 0.5 contains a remote code execution vulnerability that allows attackers to craft malicious JWT tokens with administrative privileges. Attackers can generate forged tokens with admin roles and upload custom DLL payloads to execute arbitrary commands on the target system.	9.8	More Details
CVE-2025-64155	An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4, FortiSIEM 7.1.0 through 7.1.8, FortiSIEM 7.0.0 through 7.0.4, FortiSIEM 6.7.0 through 6.7.10 may allow an attacker to execute unauthorized code or commands via crafted TCP requests.	9.8	More Details
CVE-2025-47855	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in Fortinet FortiFone 7.0.0 through 7.0.1, FortiFone 3.0.13 through 3.0.23 allows an unauthenticated attacker to obtain the device configuration via crafted HTTP or HTTPS requests.	9.8	More Details
CVE-2026-0892	Memory safety bugs present in Firefox 146 and Thunderbird 146. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 147.	9.8	More Details
CVE-2026-0884	Use-after-free in the JavaScript Engine component. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	9.8	More Details
CVE-2026-22234	OPEXUS eCasePortal before version 9.0.45.0 allows an unauthenticated attacker to navigate to the 'Attachments.aspx' endpoint, iterate through predictable values of 'formid', and download or delete all user-uploaded files, or upload new files.	9.8	More Details
CVE-2023-	Webgrind 1.1 contains a remote command execution vulnerability that allows unauthenticated attackers to inject OS commands via the dataFile parameter in index.php. Attackers can execute arbitrary system		More

54339	commands by manipulating the dataFile parameter, such as using payload '0%27%26calc.exe%26%27' to execute commands on the target system.	9.8	Details
CVE-2025-61548	SQL Injection is present on the hfInventoryDistFormID parameter in the /PSP/appNET/Store/CartV12.aspx/GetUnitPrice endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34. Unsanitized user input is incorporated directly into SQL queries without proper parameterization or escaping. This vulnerability allows remote attackers to execute arbitrary SQL commands	9.8	More Details
CVE-2025-67920	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Neo Ocular neoocular allows PHP Local File Inclusion.This issue affects Neo Ocular: from n/a through < 1.2.	9.8	More Details
CVE-2025-67913	Missing Authorization vulnerability in Aruba.it Dev Aruba HiSpeed Cache aruba-hispeed-cache allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Aruba HiSpeed Cache: from n/a through < 3.0.3.	9.8	More Details
CVE-2025-67911	Deserialization of Untrusted Data vulnerability in Tribulant Software Newsletters newsletters-lite allows Object Injection.This issue affects Newsletters: from n/a through <= 4.11.	9.8	More Details
CVE-2025-67910	Unrestricted Upload of File with Dangerous Type vulnerability in contentstudio Contentstudio contentstudio allows Upload a Web Shell to a Web Server.This issue affects Contentstudio: from n/a through <= 1.3.7.	9.8	More Details
CVE-2025-23993	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RiceTheme Felan Framework felan-framework allows SQL Injection.This issue affects Felan Framework: from n/a through <= 1.1.3.	9.8	More Details
CVE-2025-23504	Authentication Bypass Using an Alternate Path or Channel vulnerability in RiceTheme Felan Framework felan-framework allows Authentication Abuse.This issue affects Felan Framework: from n/a through <= 1.1.3.	9.8	More Details
CVE-2025-14358	Missing Authorization vulnerability in sizam REHub Framework rehub-framework allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects REHub Framework: from n/a through <= 19.9.5.	9.8	More Details
CVE-2025-14359	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in brandexponents Oshine oshin allows PHP Local File Inclusion.This issue affects Oshine: from n/a through <= 7.2.7.	9.8	More Details
CVE-2025-14360	Missing Authorization vulnerability in Kaira Blockons blockons allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Blockons: from n/a through <= 1.2.15.	9.8	More Details
CVE-2025-22728	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AmentoTech Workreap (theme's plugin) workreap allows SQL Injection.This issue affects Workreap (theme's plugin): from n/a through <= 3.3.6.	9.8	More Details
CVE-2025-14429	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove AeroLand aeroland allows PHP Local File Inclusion.This issue affects AeroLand: from n/a through <= 1.6.6.	9.8	More Details
CVE-2025-22713	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in vanquish WooCommerce Orders & Customers Exporter woocommerce-orders-ei allows SQL Injection.This issue affects WooCommerce Orders & Customers Exporter: from n/a through <= 5.4.	9.8	More Details
CVE-2025-14430	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Brook - Agency Business Creative brook allows PHP Local File Inclusion.This issue affects Brook - Agency Business Creative: from n/a through <= 2.8.9.	9.8	More Details
CVE-2025-14431	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in THEMELOGI Navian navian allows PHP Local File Inclusion.This issue affects Navian: from n/a through <= 1.5.4.	9.8	More Details
CVE-2025-22509	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in TMRW-studio Atlas atlas allows PHP Local File Inclusion.This issue affects Atlas: from n/a through <= 2.1.0.	9.8	More Details
CVE-2025-22707	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Moody tm-moody allows PHP Local File Inclusion.This issue affects Moody: from n/a through <= 2.7.3.	9.8	More Details
CVE-2025-67915	Authentication Bypass Using an Alternate Path or Channel vulnerability in Arraytics Timetics timetics allows Authentication Abuse.This issue affects Timetics: from n/a through <= 1.0.46.	9.8	More Details

CVE-2025-12550	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes OchaHouse ochahouse allows PHP Local File Inclusion.This issue affects OchaHouse: from n/a through <= 2.2.8.	9.8	More Details
CVE-2025-22712	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in QantumThemes Typify typify allows PHP Local File Inclusion.This issue affects Typify: from n/a through <= 3.0.2.	9.8	More Details
CVE-2025-12549	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in magentech Rozy - Flower Shop rozy allows PHP Local File Inclusion.This issue affects Rozy - Flower Shop: from n/a through <= 1.2.25.	9.8	More Details
CVE-2025-61246	indieka900 online-shopping-system-php 1.0 is vulnerable to SQL Injection in master/review_action.php via the prold parameter.	9.8	More Details
CVE-2025-47552	Deserialization of Untrusted Data vulnerability in Digital zoom studio DZS Video Gallery allows Object Injection.This issue affects DZS Video Gallery: from n/a through 12.37.	9.8	More Details
CVE-2026-21854	The Tarkov Data Manager is a tool to manage the Tarkov item data. Prior to 02 January 2025, an authentication bypass vulnerability in the login endpoint allows any unauthenticated user to gain full admin access to the Tarkov Data Manager admin panel by exploiting a JavaScript prototype property access vulnerability, combined with loose equality type coercion. A series of fix commits on 02 January 2025 fixed this and other vulnerabilities.	9.8	More Details
CVE-2026-22189	Panda3D versions up to and including 1.10.16 egg-mkfont contains a stack-based buffer overflow vulnerability due to use of an unbounded sprintf() call with attacker-controlled input. When constructing glyph filenames, egg-mkfont formats a user-supplied glyph pattern (-gp) into a fixed-size stack buffer without length validation. Supplying an excessively long glyph pattern string can overflow the stack buffer, resulting in memory corruption and a deterministic crash. Depending on build configuration and execution environment, the overflow may also be exploitable for arbitrary code execution.	9.8	More Details
CVE-2017-20216	FLIR Thermal Camera PT-Series firmware version 8.0.0.64 contains multiple unauthenticated remote command injection vulnerabilities in the controllerFlirSystem.php script. Attackers can execute arbitrary system commands as root by exploiting unsanitized POST parameters in the execFlirSystem() function through shell_exec() calls. Exploitation evidence was observed by the Shadowserver Foundation on 2026-01-06 (UTC).	9.8	More Details
CVE-2019-25268	NREL BEopt 2.8.0.0 contains a DLL hijacking vulnerability that allows attackers to load arbitrary libraries by tricking users into opening application files from remote shares. Attackers can exploit insecure library loading of sdl2.dll and libegl.dll by placing malicious libraries on WebDAV or SMB shares to execute unauthorized code.	9.8	More Details
CVE-2019-25282	V-SOL GPON/EPON OLT Platform v2.03 contains an open redirect vulnerability in the script that allows attackers to manipulate the 'parent' GET parameter. Attackers can craft malicious links that redirect logged-in users to arbitrary websites by exploiting improper input validation in the redirect mechanism.	9.8	More Details
CVE-2026-21875	ClipBucket v5 is an open source video sharing platform. Versions 5.5.2-#187 and below allow an attacker to perform Blind SQL Injection through the add comment section within a channel. When adding a comment within a channel, there is a POST request to the /actions/ajax.php endpoint. The obj_id parameter within the POST request to /actions/ajax.php is then used within the user_exists function of the upload/includes/classes/user.class. php file as the $id parameter. It is then used within the count function of the upload/includes/classes/db.class. php file. The $id parameter is concatenated into the query without validation or sanitization, and a user-supplied input like 1' or 1=1-- - can be used to trigger the injection. This issue does not have a fix at the time of publication.	9.8	More Details
CVE-2019-25296	The WP Cost Estimation plugin for WordPress is vulnerable to arbitrary file uploads and deletion due to missing file type validation in the lfb_upload_form and lfb_removeFile AJAX actions in versions up to, and including, 9.642. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible. Additionally, the attacker can also delete files on the server such as database configuration files, subsequently uploading their own database files.	9.8	More Details
CVE-2025-69258	A LoadLibraryEX vulnerability in Trend Micro Apex Central could allow an unauthenticated remote attacker to load an attacker-controlled DLL into a key executable, leading to execution of attacker-supplied code under the context of SYSTEM on affected installations.	9.8	More Details
CVE-2025-62877	Projects using the SUSE Virtualization (Harvester) environment may expose the OS default ssh login password if they are using the 1.5.x or 1.6.x interactive installer to either create a new cluster or add new hosts to an existing cluster. The environment is not affected if the PXE boot mechanism is utilized along with the Harvester configuration setup.	9.8	More Details
CVE-2025-	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in themesuite Automotive Listings automotive allows Blind SQL Injection.This issue affects Automotive	9.8	More

67928	Listings: from n/a through <= 18.6.		Details
CVE-2025-67924	Unrestricted Upload of File with Dangerous Type vulnerability in zozothemes Corpkit corpkit allows Upload a Web Shell to a Web Server.This issue affects Corpkit: from n/a through <= 2.0.	9.8	More Details
CVE-2025-67921	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VanKarWai Lobo lobo allows Blind SQL Injection.This issue affects Lobo: from n/a through < 2.8.6.	9.8	More Details
CVE-2025-22708	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Mitech mitech allows PHP Local File Inclusion.This issue affects Mitech: from n/a through <= 2.3.4.	9.8	More Details
CVE-2025-12543	A flaw was found in the Undertow HTTP server core, which is used in WildFly, JBoss EAP, and other Java applications. The Undertow library fails to properly validate the Host header in incoming HTTP requests.As a result, requests containing malformed or malicious Host headers are processed without rejection, enabling attackers to poison caches, perform internal network scans, or hijack user sessions.	9.6	More Details
CVE-2026-22794	Appsmith is a platform to build admin panels, internal tools, and dashboards. Prior to 1.93, the server uses the Origin value from the request headers as the email link baseUrl without validation. If an attacker controls the Origin, password reset / email verification links in emails can be generated pointing to the attacker’s domain, causing authentication tokens to be exposed and potentially leading to account takeover. This vulnerability is fixed in 1.93.	9.6	More Details
CVE-2026-0500	Due to the usage of vulnerable third party component in SAP Wily Introscope Enterprise Manager (WorkStation), an unauthenticated attacker could create a malicious JNLP (Java Network Launch Protocol) file accessible by a public facing URL. When a victim clicks on the URL the accessed Wily Introscope Server could execute OS commands on the victim's machine. This could completely compromising confidentiality, integrity and availability of the system.	9.6	More Details
CVE-2026-22783	Iris is a web collaborative platform that helps incident responders share technical details during investigations. Prior to 2.4.24, the DFIR-IRIS datastore file management system has a vulnerability where mass assignment of the file_local_name field combined with path trust in the delete operation enables authenticated users to delete arbitrary filesystem paths. The vulnerability manifests through a three-step attack chain: authenticated users upload a file to the datastore, update the file's file_local_name field to point to an arbitrary filesystem path through mass assignment, then trigger the delete operation which removes the target file without path validation. This vulnerability is fixed in 2.4.24.	9.6	More Details
CVE-2025-67146	Multiple SQL Injection vulnerabilities exist in AbhishekMali21 GYM-MANAGEMENT-SYSTEM 1.0 via the 'name' parameter in (1) member_search.php, (2) trainer_search.php, and (3) gym_search.php, and via the 'id' parameter in (4) payment_search.php. An unauthenticated remote attacker can exploit these issues to inject malicious SQL commands, leading to unauthorized data extraction, authentication bypass, or modification of database contents.	9.4	More Details
CVE-2025-66916	The snailjob component in RuoYi-Vue-Plus versions 5.5.1 and earlier, interface /snail-job/workflow/check-node-expression can execute QLExpress expressions, but it does not filter user input, allowing attackers to use the File class to perform arbitrary file reading and writing.	9.4	More Details
CVE-2026-21891	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In versions up to and including 1.5.0, the application checks the validity of the username but appears to skip, misinterpret, or incorrectly validate the password when the provided username matches a known system service account. The application's login function fails to properly handle the password validation result for these users, effectively granting authenticated access to anyone who knows one of these common usernames and provides any password. As of time of publication, no known patched versions are available.	9.4	More Details
CVE-2025-68717	KAYSUS KS-WR3600 routers with firmware 1.0.5.9.1 allow authentication bypass during session validation. If any user is logged in, endpoints such as /cgi-bin/system-tool accept unauthenticated requests with empty or invalid session values. This design flaw lets attackers piggyback on another user's active session to retrieve sensitive configuration data or execute privileged actions without authentication.	9.4	More Details
CVE-2026-21876	The OWASP core rule set (CRS) is a set of generic attack detection rules for use with compatible web application firewalls. Prior to versions 4.22.0 and 3.3.8, the current rule 922110 has a bug when processing multipart requests with multiple parts. When the first rule in a chain iterates over a collection (like `MULTIPART_PART_HEADERS`), the capture variables (`TX:0`, `TX:1`) get overwritten with each iteration. Only the last captured value is available to the chained rule, which means malicious charsets in earlier parts can be missed if a later part has a legitimate charset. Versions 4.22.0 and 3.3.8 patch the issue.	9.3	More Details
CVE-2025-32303	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mojoomla WPCHURCH allows Blind SQL Injection.This issue affects WPCHURCH: from n/a through 2.7.0.	9.3	More Details
	The Tarkov Data Manager is a tool to manage the Tarkov item data. Prior to 02 January 2025, a reflected		

CVE-2026-21855	Cross Site Scripting (XSS) vulnerability in the toast notification system allows any attacker to execute arbitrary JavaScript in the context of a victim's browser session by crafting a malicious URL. A series of fix commits on 02 January 2025 fixed this and other vulnerabilities.	9.3	More Details
CVE-2025-11250	Zohocorp ManageEngine ADSelfService Plus versions before 6519 are vulnerable to Authentication Bypass due to improper filter configurations.	9.1	More Details
CVE-2025-68637	The Uniffle HTTP client is configured to trust all SSL certificates and disables hostname verification by default. This insecure configuration exposes all REST API communication between the Uniffle CLI/client and the Uniffle Coordinator service to potential Man-in-the-Middle (MITM) attacks. This issue affects all versions from before 0.10.0. Users are recommended to upgrade to version 0.10.0, which fixes the issue.	9.1	More Details
CVE-2026-0498	SAP S/4HANA (Private Cloud and On-Premise) allows an attacker with admin privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code/OS commands into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of the system.	9.1	More Details
CVE-2025-68715	An issue was discovered in Panda Wireless PWRU0 devices with firmware 2.2.9 that exposes multiple HTTP endpoints (/goform/setWan, /goform/setLan, /goform/wirelessBasic) that do not enforce authentication. A remote unauthenticated attacker can modify WAN, LAN, and wireless settings directly, leading to privilege escalation and denial of service.	9.1	More Details
CVE-2025-69222	LibreChat is a ChatGPT clone with additional features. Version 0.8.1-rc2 is prone to a server-side request forgery (SSRF) vulnerability due to missing restrictions of the Actions feature in the default configuration. LibreChat enables users to configure agents with predefined instructions and actions that can interact with remote services via OpenAPI specifications, supporting various HTTP methods, parameters, and authentication methods including custom headers. By default, there are no restrictions on accessible services, which means agents can also access internal components like the RAG API included in the default Docker Compose setup. This issue is fixed in version 0.8.1-rc2.	9.1	More Details
CVE-2025-14741	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to missing authorization to unauthorized data modification and deletion due to a missing capability check on the 'delete_object' function in all versions up to, and including, 3.28.25. This makes it possible for unauthenticated attackers to delete arbitrary posts, pages, products, taxonomy terms, and user accounts.	9.1	More Details
CVE-2025-22726	Server-Side Request Forgery (SSRF) vulnerability in _nK nK Themes Helper nk-themes-helper allows Server Side Request Forgery.This issue affects nK Themes Helper: from n/a through <= 1.7.9.	9.1	More Details
CVE-2025-61546	There is an issue on the /PSP/appNET/Store/CartV12.aspx/GetUnitPrice endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34 that enables remote attacker to create financial discrepancies by purchasing items with a negative quantity. This vulnerability is possible due to reliance on client-side input validation controls.	9.1	More Details
CVE-2026-21881	Kanboard is project management software focused on Kanban methodology. Versions 1.2.48 and below is vulnerable to a critical authentication bypass when REVERSE_PROXY_AUTH is enabled. The application blindly trusts HTTP headers for user authentication without verifying the request originated from a trusted reverse proxy. An attacker can impersonate any user, including administrators, by simply sending a spoofed HTTP header. This issue is fixed in version 1.2.49.	9.1	More Details
CVE-2025-14829	The E-xact | Hosted Payment | WordPress plugin through 2.0 is vulnerable to arbitrary file deletion due to insufficient file path validation. This makes it possible for unauthenticated attackers to delete arbitrary files on the server.	9.1	More Details
CVE-2026-22600	OpenProject is an open-source, web-based project management software. A Local File Read (LFR) vulnerability exists in the work package PDF export functionality of OpenProject prior to version 16.6.4. By uploading a specially crafted SVG file (disguised as a PNG) as a work package attachment, an attacker can exploit the backend image processing engine (ImageMagick). When the work package is exported to PDF, the backend attempts to resize the image, triggering the ImageMagick text: coder. This allows an attacker to read arbitrary local files that the application user has permissions to access (e.g., /etc/passwd, all project configuration files, private project data, etc.). The attack requires permissions to upload attachments to a container that can be exported to PDF, such as a work package. The issue has been patched in version 16.6.4. Those who are unable to upgrade may apply the patch manually.	9.1	More Details
CVE-2025-61686	React Router is a router for React. In @react-router/node versions 7.0.0 through 7.9.3, @remix-run/deno prior to version 2.17.2, and @remix-run/node prior to version 2.17.2, if createFileSessionStorage() is being used from @react-router/node (or @remix-run/node/@remix-run/deno in Remix v2) with an unsigned cookie, it is possible for an attacker to cause the session to try to read/write from a location outside the specified session file directory. The success of the attack would depend on the permissions of the web server process to access those files. Read files cannot be returned directly to the attacker. Session file reads would only succeed if the file matched the expected session file format. If the file matched the session file format, the data would be populated into the server side session but not	9.1	More Details

	directly returned to the attacker unless the application logic returned specific session information. This issue has been patched in @react-router/node version 7.9.4, @remix-run/deno version 2.17.2, and @remix-run/node version 2.17.2.		
CVE-2026-22252	LibreChat is a ChatGPT clone with additional features. Prior to v0.8.2-rc2, LibreChat's MCP stdio transport accepts arbitrary commands without validation, allowing any authenticated user to execute shell commands as root inside the container through a single API request. This vulnerability is fixed in v0.8.2-rc2.	9.1	More Details
CVE-2026-0491	SAP Landscape Transformation allows an attacker with admin privileges to exploit a vulnerability in the function module exposed via RFC. This flaw enables the injection of arbitrary ABAP code/OS commands into the system, bypassing essential authorization checks. This vulnerability effectively functions as a backdoor, creating the risk of full system compromise, undermining the confidentiality, integrity and availability of the system.	9.1	More Details
CVE-2025-51567	A SQL Injection was found in the /exam/user/profile.php page of kashipara Online Exam System V1.0, which allows remote attackers to execute arbitrary SQL command to get unauthorized database access via the rname, rcollage, rnumber, rgender and rpassword parameters in a POST HTTP request.	9.1	More Details
CVE-2025-56425	An issue was discovered in the AppConnector component version 10.10.0.183 and earlier of enaio 10.10, in the AppConnector component version 11.0.0.183 and earlier of enaio 11.0, and in the AppConnctor component version 11.10.0.183 and earlier of enaio 11.10. The vulnerability allows authenticated remote attackers to inject arbitrary SMTP commands via crafted input to the /osrest/api/organization/sendmail endpoint	9.1	More Details
CVE-2025-59468	This vulnerability allows a Backup Administrator to perform remote code execution (RCE) as the postgres user by sending a malicious password parameter.	9.0	More Details
CVE-2025-59469	This vulnerability allows a Backup or Tape Operator to write files as root.	9.0	More Details
CVE-2025-59470	This vulnerability allows a Backup Operator to perform remote code execution (RCE) as the postgres user by sending a malicious interval or order parameter.	9.0	More Details
CVE-2025-12548	A flaw was found in Eclipse Che che-machine-exec. This vulnerability allows unauthenticated remote arbitrary command execution and secret exfiltration (SSH keys, tokens, etc.) from other users' Developer Workspace containers, via an unauthenticated JSON-RPC / websocket API exposed on TCP port 3333.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-0838	A security flaw has been discovered in UTT 进取 520W 1.7.7-180627. This impacts the function strcpy of the file /goform/ConfigWirelessBase. Performing a manipulation of the argument ssid results in buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2022-50916	e107 CMS version 3.2.1 contains a file upload vulnerability that allows authenticated administrators to override server files through the Media Manager import functionality. Attackers can exploit the upload mechanism by manipulating the upload URL parameter to overwrite existing files like top.php in the web application directory.	8.8	More Details
CVE-2026-0854	Certain DVR/NVR models developed by Merit LILIN has a OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the device.	8.8	More Details
CVE-2026-0882	Use-after-free in the IPC component. This vulnerability affects Firefox < 147, Firefox ESR < 115.32, and Firefox ESR < 140.7.	8.8	More Details
CVE-2025-31643	Incorrect Privilege Assignment vulnerability in Dasinfomedia WPCHURCH allows Privilege Escalation.This issue affects WPCHURCH: from n/a through 2.7.0.	8.8	More Details
CVE-2022-50911	Bitrix24 contains an authenticated remote code execution vulnerability that allows logged-in attackers to execute arbitrary system commands through the PHP command line admin interface. Attackers can leverage the vulnerability by sending crafted POST requests to the administrative endpoint with system commands to execute code with the web application's privileges.	8.8	More Details
CVE-	Algo 8028 Control Panel version 3.3.3 contains a command injection vulnerability in the fm-data.lua endpoint		

2022-50909	that allows authenticated attackers to execute arbitrary commands. Attackers can exploit the insecure 'source' parameter by injecting commands that are executed with root privileges, enabling remote code execution through a crafted POST request.	8.8	More Details
CVE-2025-69194	A security issue was discovered in GNU Wget2 when handling Metalink documents. The application fails to properly validate file paths provided in Metalink <file name> elements. An attacker can abuse this behavior to write files to unintended locations on the system. This can lead to data loss or potentially allow further compromise of the user’s environment.	8.8	More Details
CVE-2022-50907	e107 CMS version 3.2.1 contains a file upload vulnerability that allows authenticated administrative users to bypass upload restrictions and execute PHP files. Attackers can upload malicious PHP files to parent directories by manipulating the upload URL parameter, enabling remote code execution through the Media Manager import feature.	8.8	More Details
CVE-2026-0839	A weakness has been identified in UTT 进取 520W 1.7.7-180627. Affected is the function strcpy of the file /goform/APSecurity. Executing a manipulation of the argument wepkey1 can lead to buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-15158	The WP Enable WebP plugin for WordPress is vulnerable to arbitrary file uploads due to improper file type validation in the 'wpse_file_and_ext_webp' function in all versions up to, and including, 1.0. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-69264	pnpm is a package manager. Versions 10.0.0 through 10.25 allow git-hosted dependencies to execute arbitrary code during pnpm install, circumventing the v10 security feature "Dependency lifecycle scripts execution disabled by default". While pnpm v10 blocks postinstall scripts via the onlyBuiltDependencies mechanism, git dependencies can still execute prepare, prepublish, and prepack scripts during the fetch phase, enabling remote code execution without user consent or approval. This issue is fixed in version 10.26.0.	8.8	More Details
CVE-2019-25289	SmartLiving SmartLAN <=6.x contains an authenticated remote command injection vulnerability in the web.cgi binary through the 'par' POST parameter with the 'testemail' module. Attackers can exploit the unsanitized parameter and system() function call to execute arbitrary system commands with root privileges using default credentials.	8.8	More Details
CVE-2022-50898	NanoCMS 0.4 contains an authenticated file upload vulnerability that allows remote code execution through unvalidated page content creation. Authenticated attackers can upload PHP files with arbitrary code to the server's pages directory by exploiting the page creation mechanism without proper input sanitization.	8.8	More Details
CVE-2026-0840	A security vulnerability has been detected in UTT 进取 520W 1.7.7-180627. Affected by this vulnerability is the function strcpy of the file /goform/formConfigNoticeConfig. The manipulation of the argument timestart leads to buffer overflow. It is possible to initiate 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.	8.8	More Details
CVE-2026-0855	Certain IP Camera models developed by Merit LILIN has a OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the device.	8.8	More Details
CVE-2026-21683	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `icStatusCMM::CIccEvalCompare::EvaluateProfile()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2022-50806	4images 1.9 contains a remote command execution vulnerability that allows authenticated administrators to inject reverse shell code through template editing functionality. Attackers can save malicious code in the template and execute arbitrary commands by accessing a specific categories.php endpoint with a crafted cat_id parameter.	8.8	More Details
CVE-2025-46068	An issue in Automai Director v.25.2.0 allows a remote attacker to execute arbitrary code via the update mechanism	8.8	More Details
CVE-2026-0841	A vulnerability was detected in UTT 进取 520W 1.7.7-180627. Affected by this issue is the function strcpy of the file /goform/formPictureUrl. The manipulation of the argument importpictureurl results in buffer overflow. It is possible to launch the attack 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-2026-22861	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Prior to 2.3.1.2, There is a heap-based buffer overflow in SIccCalcOp::Describe() at IccProfLib/IccMpeCalc.cpp. This vulnerability affects users of the iccDEV library who process ICC color profiles. The vulnerability is fixed in 2.3.1.2.	8.8	More Details

CVE-2026-21688	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `SIccCalcOp::ArgsPushed()` at `IccProfLib/IccMpeCalc.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2025-36640	A vulnerability has been identified in the installation/uninstallation of the Nessus Agent Tray App on Windows Hosts which could lead to escalation of privileges.	8.8	More Details
CVE-2026-0880	Sandbox escape due to integer overflow in the Graphics component. This vulnerability affects Firefox < 147, Firefox ESR < 115.32, and Firefox ESR < 140.7.	8.8	More Details
CVE-2025-66001	NeuVector supports login authentication through OpenID Connect. However, the TLS verification (which verifies the remote server's authenticity and integrity) for OpenID Connect is not enforced by default. As a result this may expose the system to man-in-the-middle (MITM) attacks.	8.8	More Details
CVE-2026-22047	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a heap-buffer-overflow vulnerability in `SIccCalcOp::Describe()` at `IccProfLib/IccMpeCalc.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2026-22046	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a heap-buffer-overflow vulnerability in `CIccProfileXml::ParseBasic()` at `IccXML/IccLibXML/IccProfileXml.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2026-21693	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `CIccSegmentedCurveXml::ToXml()` at `IccXML/IccLibXML/IccMpeXml.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2026-21692	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `ToXmlCurve()` at `IccXML/IccLibXML/IccMpeXml.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2026-20963	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2025-15499	A vulnerability has been found in Sangfor Operation and Maintenance Management System up to 3.0.8. This vulnerability affects the function uploadCN of the file VersionController.java. The manipulation of the argument filename leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-13774	A vulnerability exists in Progress Flowmon ADS versions prior to 12.5.4 and 13.0.1 where an SQL injection vulnerability allows authenticated users to execute unintended SQL queries and commands.	8.8	More Details
CVE-2025-40942	A vulnerability has been identified in TeleControl Server Basic (All versions < V3.1.2.4). Affected application contains a local privilege escalation vulnerability that could allow an attacker to run arbitrary code with elevated privileges.	8.8	More Details
CVE-2026-21679	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to heap-buffer-overflow in CIccLocalizedUnicode::GetText(). This issue has been patched in version 2.3.1.2.	8.8	More Details
CVE-2025-67926	Missing Authorization vulnerability in Shahjahan Jewel Fluent Support fluent-support allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent Support: from n/a through <= 1.10.4.	8.8	More Details
CVE-2026-21638	A malicious actor in Wi-Fi range of the affected product could leverage a vulnerability in the airMAX Wireless Protocol to achieve a remote code execution (RCE) within the affected product. Affected Products: UBB-XG (Version 1.2.2 and earlier) UDB-Pro/UDB-Pro-Sector (Version 1.4.1 and earlier) UBB (Version 3.1.5 and earlier) Mitigation: Update your UBB-XG to Version 1.2.3 or later. Update your UDB-Pro/UDB-Pro-Sector to Version 1.4.2 or later. Update your UBB to Version 3.1.7 or later.	8.8	More Details

CVE-2026-22256	Salvo is a Rust web backend framework. Prior to version 0.88.1, the function list_html generate an file view of a folder which include a render of the current path, in which its inserted in the HTML without proper sanitation, this leads to reflected XSS using the fact that request path is decoded and normalized in the matching stage but not is inserted raw in the html view (current.path), the only constraint here is for the root path (eg. /files in the PoC example) to have a sub directory (e.g common ones styles/scripts/etc...) so that the matching return the list HTML page instead of the Not Found page. This issue has been patched in version 0.88.1.	8.8	More Details
CVE-2026-0628	Insufficient policy enforcement in WebView tag in Google Chrome prior to 143.0.7499.192 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: High)	8.8	More Details
CVE-2026-22685	DevToys is a desktop app for developers. In versions from 2.0.0.0 to before 2.0.9.0, a path traversal vulnerability exists in the DevToys extension installation mechanism. When processing extension packages (NUPKG archives), DevToys does not sufficiently validate file paths contained within the archive. A malicious extension package could include crafted file entries such as ../../.../target-file, causing the extraction process to write files outside the intended extensions directory. This flaw enables an attacker to overwrite arbitrary files on the user's system with the privileges of the DevToys process. Depending on the environment, this may lead to code execution, configuration tampering, or corruption of application or system files. This issue has been patched in version 2.0.9.0.	8.8	More Details
CVE-2026-22812	OpenCode is an open source AI coding agent. Prior to 1.0.216, OpenCode automatically starts an unauthenticated HTTP server that allows any local process (or any website via permissive CORS) to execute arbitrary shell commands with the user's privileges. This vulnerability is fixed in 1.0.216.	8.8	More Details
CVE-2026-22257	Salvo is a Rust web backend framework. Prior to version 0.88.1, the function list_html generates a file view of a folder without sanitizing the files or folders names, this may potentially lead to XSS in cases where a website allow the access to public files using this feature and anyone can upload a file. This issue has been patched in version 0.88.1.	8.8	More Details
CVE-2025-61939	An unused function in MicroServer can start a reverse SSH connection to a vendor registered domain, without mutual authentication. An attacker on the local network with admin access to the web server, and the ability to manipulate DNS responses, can redirect the SSH connection to an attacker controlled device.	8.8	More Details
CVE-2026-0492	SAP HANA database is vulnerable to privilege escalation allowing an attacker with valid credentials of any user to switch to another user potentially gaining administrative access. This exploit could result in a total compromise of the system's confidentiality, integrity, and availability.	8.8	More Details
CVE-2017-20215	FLIR Thermal Camera FC-S/PT firmware version 8.0.0.64 contains an authenticated OS command injection vulnerability that allows attackers to execute shell commands with root privileges. Authenticated attackers can inject arbitrary shell commands through unvalidated input parameters to gain complete control of the thermal camera system.	8.8	More Details
CVE-2026-22255	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a heap-buffer-overflow vulnerability in `CIccCLUT::Init()` at `IccProfLib/IccTagLut.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2022-50936	WBCE CMS version 1.5.2 contains an authenticated remote code execution vulnerability that allows attackers to upload malicious droplets through the admin panel. Authenticated attackers can exploit the droplet upload functionality in the admin tools to create and execute arbitrary PHP code by crafting a specially designed zip file payload.	8.8	More Details
CVE-2022-50934	Wing FTP Server versions 4.3.8 and below contain an authenticated remote code execution vulnerability that allows attackers to execute arbitrary PowerShell commands through the admin interface. Attackers can leverage a crafted Lua script payload with base64-encoded PowerShell to establish a reverse TCP shell by authenticating and sending a malicious request to the admin panel.	8.8	More Details
CVE-2026-22771	Envoy Gateway is an open source project for managing Envoy Proxy as a standalone or Kubernetes-based application gateway. Prior to 1.5.7 and 1.6.2, EnvoyExtensionPolicy Lua scripts executed by Envoy proxy can be used to leak the proxy's credentials. These credentials can then be used to communicate with the control plane and gain access to all secrets that are used by Envoy proxy, e.g. TLS private keys and credentials used for downstream and upstream communication. This vulnerability is fixed in 1.5.7 and 1.6.2.	8.8	More Details
CVE-2026-21682	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a heap-buffer-overflow in `CIccXmlArrayType::ParseText()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	8.8	More Details
CVE-2025-	An unauthenticated remote attacker can trick a high privileged user into uploading a malicious payload via the config-upload endpoint, leading to code injection as root. This results in a total loss of confidentiality,	8.8	More

41717	availability and integrity due to improper control of code generation ('Code Injection').		Details
CVE-2026-21869	llama.cpp is an inference of several LLM models in C/C++. In commits 55d4206c8 and prior, the n_discard parameter is parsed directly from JSON input in the llama.cpp server's completion endpoints without validation to ensure it's non-negative. When a negative value is supplied and the context fills up, llama_memory_seq_rm/add receives a reversed range and negative offset, causing out-of-bounds memory writes in the token evaluation loop. This deterministic memory corruption can crash the process or enable remote code execution (RCE). There is no fix at the time of publication.	8.8	More Details
CVE-2026-0836	A vulnerability was determined in UTT 进取 520W 1.7.7-180627. The impacted element is the function strcpy of the file /goform/formConfigFastDirectionW. This manipulation of the argument ssid causes buffer overflow. Remote exploitation of the attack is possible. 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-2025-68719	KAYSUS KS-WR3600 routers with firmware 1.0.5.9.1 mishandle configuration management. Once any user is logged in and maintains an active session, an attacker can directly query the backup endpoint and download a full configuration archive. This archive contains sensitive files such as /etc/shadow, enabling credential recovery and potential full compromise of the device.	8.8	More Details
CVE-2025-66177	There is a Stack overflow Vulnerability in the device Search and Discovery feature of Hikvision NVR/DVR/CVR/IPC models. If exploited, an attacker on the same local area network (LAN) could cause the device to malfunction by sending specially crafted packets to an unpatched device.	8.8	More Details
CVE-2026-20868	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-4676	Incorrect Implementation of Authentication Algorithm vulnerability in ABB WebPro SNMP Card PowerValue, ABB WebPro SNMP Card PowerValue UL.This issue affects WebPro SNMP Card PowerValue: through 1.1.8.K; WebPro SNMP Card PowerValue UL: through 1.1.8.K.	8.8	More Details
CVE-2026-20947	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2026-0837	A vulnerability was identified in UTT 进取 520W 1.7.7-180627. This affects the function strcpy of the file /goform/formFireWall. Such manipulation of the argument GroupName leads to buffer overflow. 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.	8.8	More Details
CVE-2025-66176	There is a Stack overflow Vulnerability in the device Search and Discovery feature of Hikvision Access Control Products. If exploited, an attacker on the same local area network (LAN) could cause the device to malfunction by sending specially crafted packets to an unpatched device.	8.8	More Details
CVE-2025-63611	Cross-Site Scripting in phpgurukul Hostel Management System v2.1 user-provided complaint fields (Explain the Complaint) submitted via /register-complaint.php are stored and rendered unescaped in the admin viewer (/admin/complaint-details.php?cid=<id>). When an administrator opens the complaint, injected HTML/JavaScript executes in the admin's browser.	8.7	More Details
CVE-2025-9222	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2.2 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed an authenticated user to achieve stored cross-site scripting by exploiting GitLab Flavored Markdown.	8.7	More Details
CVE-2026-0719	A flaw was identified in the NTLM authentication handling of the libsoup HTTP library, used by GNOME and other applications for network communication. When processing extremely long passwords, an internal size calculation can overflow due to improper use of signed integers. This results in incorrect memory allocation on the stack, followed by unsafe memory copying. As a result, applications using libsoup may crash unexpectedly, creating a denial-of-service risk.	8.6	More Details
CVE-2026-21280	Illustrator versions 29.8.3, 30.0 and earlier are affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. If the application uses a search path to locate critical resources such as programs, an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue requires user interaction in that a victim must open a malicious file and scope is changed.	8.6	More Details
CVE-2026-21267	Dreamweaver Desktop versions 21.6 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an attacker. Exploitation of this issue requires user interaction in that a victim must open a malicious file and scope is changed.	8.6	More Details
CVE-2026-21268	Dreamweaver Desktop versions 21.6 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file and scope is changed.	8.6	More Details

CVE-2026-21271	Dreamweaver Desktop versions 21.6 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file and scope is changed.	8.6	More Details
CVE-2026-21272	Dreamweaver Desktop versions 21.6 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system write. An attacker could leverage this vulnerability to manipulate or inject malicious data into files on the system. Exploitation of this issue requires user interaction in that a victim must open a malicious file and scope is changed.	8.6	More Details
CVE-2025-64091	This vulnerability allows authenticated attackers to execute commands via the NTP-configuration of the device.	8.6	More Details
CVE-2025-13371	The MoneySpace plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.13.9. This is due to the plugin storing full payment card details (PAN, card holder name, expiry month/year, and CVV) in WordPress post_meta using base64_encode(), and then embedding these values into the publicly accessible mspaylink page's inline JavaScript without any authentication or authorization check. This makes it possible for unauthenticated attackers who know or can guess an order_id to access the mspaylink endpoint and retrieve full credit card numbers and CVV codes directly from the HTML/JS response, constituting a severe PCI-DSS violation.	8.6	More Details
CVE-2025-66698	An issue in Semantic machines v5.4.8 allows attackers to bypass authentication via sending a crafted HTTP request to various API endpoints.	8.6	More Details
CVE-2025-14025	A flaw was found in Ansible Automation Platform (AAP). Read-only scoped OAuth2 API Tokens in AAP, are enforced at the Gateway level for Gateway-specific operations. However, this vulnerability allows read-only tokens to perform write operations on backend services (e.g., Controller, Hub, EDA). If this flaw were exploited, an attacker‘s capabilities would only be limited by role based access controls (RBAC).	8.5	More Details
CVE-2026-20952	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2022-50914	EaseUS Data Recovery 15.1.0.0 contains an unquoted service path vulnerability in the EaseUS UPDATE SERVICE executable. Attackers can exploit the unquoted path to inject and execute malicious code with elevated LocalSystem privileges.	8.4	More Details
CVE-2022-50915	PTPublisher 2.3.4 contains an unquoted service path vulnerability in the PTProtect service that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\Primera Technology\PTPublisher\UsbFlashDongleService.exe' to inject malicious executables and gain system-level access.	8.4	More Details
CVE-2022-50933	Cain & Abel 4.9.56 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted binary path to inject malicious executables that will be launched with LocalSystem permissions.	8.4	More Details
CVE-2022-50917	ProtonVPN 1.26.0 contains an unquoted service path vulnerability in its WireGuard service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path by placing malicious executables in specific file system locations to gain elevated privileges during service startup.	8.4	More Details
CVE-2025-68716	KAYSUS KS-WR3600 routers with firmware 1.0.5.9.1 enable the SSH service enabled by default on the LAN interface. The root account is configured with no password, and administrators cannot disable SSH or enforce authentication via the CLI or web GUI. This allows any LAN-adjacent attacker to trivially gain root shell access and execute arbitrary commands with full privileges.	8.4	More Details
CVE-2022-50920	Sandboxie-Plus 5.50.2 contains an unquoted service path vulnerability in the SbieSvc Windows service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path to inject malicious executables that will be run with LocalSystem privileges during service startup.	8.4	More Details
CVE-2026-20953	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2022-50918	VIVE Runtime Service 1.0.0.4 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path by placing malicious executables in specific system directories to gain LocalSystem access during service startup.	8.4	More Details
CVE-	Wondershare UBackit 2.0.5 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted path		More

2022-50904	in the wsbackup service to inject malicious executables that would run with LocalSystem permissions during service startup.	8.4	Details
CVE-2022-50921	WOW21 5.0.1.9 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path to inject malicious executables that will be launched with LocalSystem permissions during service startup.	8.4	More Details
CVE-2022-50923	Cobian Backup 0.9 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path in the CobianReflectorService to inject malicious code that will execute with LocalSystem permissions during service startup.	8.4	More Details
CVE-2022-50924	Private Internet Access 3.3 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious code that would execute with LocalSystem permissions during service startup.	8.4	More Details
CVE-2022-50928	BlueSoleilCS 5.4.277 contains an unquoted service path vulnerability in its Windows service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path in 'C:\Program Files\IVT Corporation\BlueSoleil\BlueSoleilCS.exe' to inject malicious executables and escalate privileges.	8.4	More Details
CVE-2022-50929	Connectify Hotspot 2018 contains an unquoted service path vulnerability in its ConnectifyService executable that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\Connectify\ConnectifyService.exe' to inject malicious executables and escalate privileges.	8.4	More Details
CVE-2026-0507	Due to an OS Command Injection vulnerability in SAP Application Server for ABAP and SAP NetWeaver RFCSDK, an authenticated attacker with administrative access and adjacent network access could upload specially crafted content to the server. If processed by the application, this content enables execution of arbitrary operating system commands. Successful exploitation could lead to full compromise of the system's confidentiality, integrity, and availability.	8.4	More Details
CVE-2025-47345	Cryptographic issue may occur while encrypting license data.	8.4	More Details
CVE-2022-50913	ITeC ITeCProteccioAppServer contains an unquoted service path vulnerability that allows local attackers to execute code with elevated system privileges. Attackers can insert a malicious executable in the service path to gain elevated access during service restart or system reboot.	8.4	More Details
CVE-2022-50902	Wondershare FamiSafe 1.0 contains an unquoted service path vulnerability in the FSService that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\Wondershare\FamiSafe\ to inject malicious code that would run with LocalSystem permissions during service startup.	8.4	More Details
CVE-2022-50693	Splashtop 8.71.12001.0 contains an unquoted service path vulnerability in the Splashtop Software Updater Service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files (x86)\Splashtop\Splashtop Software Updater\ to inject malicious executables and escalate privileges.	8.4	More Details
CVE-2023-53984	Clevo HotKey Clipboard 2.1.0.6 contains an unquoted service path vulnerability in the HKClipSvc service that allows local non-privileged users to potentially execute code with system privileges. Attackers can exploit the misconfigured service path to inject and execute arbitrary code by placing malicious executables in specific file system locations.	8.4	More Details
CVE-2023-54338	Tftpd32 SE 4.60 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious executables that will be run with system-level permissions.	8.4	More Details
CVE-2023-54336	Mediconta 3.7.27 contains an unquoted service path vulnerability in the servermedicontservice that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\medicont3\ to inject malicious code that would execute with LocalSystem permissions during service startup.	8.4	More Details
CVE-2019-25231	devolo dLAN Cockpit 4.3.1 contains an unquoted service path vulnerability in the 'DevoloNetworkService' that allows local non-privileged users to potentially execute arbitrary code. Attackers can exploit the insecure service path configuration by inserting malicious code in the system root path to execute with elevated privileges during application startup or system reboot.	8.4	More Details
CVE-2026-20944	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to execute code locally.	8.4	More Details

CVE-2023-54331	Outline 1.6.0 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted service path in the OutlineService executable to inject malicious code that will be executed with LocalSystem permissions.	8.4	More Details
CVE-2022-50903	Wondershare MobileTrans 3.5.9 contains an unquoted service path vulnerability in the ElevationService that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted path by placing malicious executables in specific filesystem locations that will be executed with LocalSystem permissions during service startup.	8.4	More Details
CVE-2022-50930	Emerson PAC Machine Edition 9.80 contains an unquoted service path vulnerability in the TrapiServer service that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious code that would execute with LocalSystem permissions during service startup.	8.4	More Details
CVE-2022-50808	CoolerMaster MasterPlus 1.8.5 contains an unquoted service path vulnerability in the MPService that allows local attackers to execute code with elevated system privileges. Attackers can drop a malicious executable in the service path and trigger code execution during service startup or system reboot.	8.4	More Details
CVE-2025-13444	OS Command Injection Remote Code Execution Vulnerability in API in Progress LoadMaster allows an authenticated attacker with “User Administration” permissions to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in the API input parameters	8.4	More Details
CVE-2022-50938	CONTPAQi AdminPAQ 14.0.0 contains an unquoted service path vulnerability in the AppKeyLicenseServer service running with LocalSystem privileges. Attackers can exploit the unquoted path to inject malicious code in the service binary path, potentially executing arbitrary code with elevated system privileges during service startup.	8.4	More Details
CVE-2022-50900	Wondershare Dr.Fone 12.0.18 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with elevated system privileges. Attackers can exploit the misconfigured service path to insert malicious code that will be executed with LocalSystem permissions during service startup.	8.4	More Details
CVE-2025-13447	OS Command Injection Remote Code Execution Vulnerability in API in Progress LoadMaster allows an authenticated attacker with “User Administration” permissions to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in the API input parameters	8.4	More Details
CVE-2022-50901	Wondershare Dr.Fone 11.4.9 contains an unquoted service path vulnerability in the DFWSIDService that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files (x86)\Wondershare\Wondershare Dr.Fone\ to inject malicious executables that would run with LocalSystem privileges.	8.4	More Details
CVE-2022-50931	TeamSpeak 3.5.6 contains an insecure file permissions vulnerability that allows local attackers to replace executable files with malicious binaries. Attackers can replace system executables like ts3client_win32.exe with custom files to potentially gain SYSTEM or Administrator-level access.	8.4	More Details
CVE-2023-54333	Social-Share-Buttons 2.2.3 contains a critical SQL injection vulnerability in the project_id parameter that allows attackers to manipulate database queries. Attackers can exploit this vulnerability by sending crafted POST requests with malicious SQL payloads to retrieve and potentially steal entire database contents.	8.2	More Details
CVE-2026-22788	WebErpMesv2 is a Resource Management and Manufacturing execution system Web for industry. Prior to 1.19, the WebErpMesV2 application exposes multiple sensitive API endpoints without authentication middleware. An unauthenticated remote attacker can read business-critical data including companies, quotes, orders, tasks, and whiteboards. Limited write access allows creation of company records and full manipulation of collaboration whiteboards. This vulnerability is fixed in 1.19.	8.2	More Details
CVE-2023-54340	WorkOrder CMS 0.1.0 contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login by manipulating username and password parameters. Attackers can inject malicious SQL queries using techniques like OR '1'='1' and stacked queries to access database information or execute administrative commands.	8.2	More Details
CVE-2023-36331	Incorrect access control in the /member/orderList API of xmall v1.1 allows attackers to arbitrarily access other users' order details via manipulation of the query parameter userId.	8.2	More Details
CVE-2025-67070	A vulnerability exists in Intelbras CFTV IP NVD 9032 R Ftd V2.800.00IB00C.0.T, which allows an unauthenticated attacker to bypass the multi-factor authentication (MFA) mechanism during the password recovery process. This results in the ability to change the admin password and gain full access to the administrative panel.	8.2	More Details
CVE-2026-0656	The iPaymu Payment Gateway for WooCommerce plugin for WordPress is vulnerable to Missing Authentication in all versions up to, and including, 2.0.2 via the 'check_ipaymu_response' function. This is due to the plugin not validating webhook request authenticity through signature verification or origin checks. This makes it possible for unauthenticated attackers to mark WooCommerce orders as paid by sending crafted POST requests to the webhook endpoint without any payment occurring, as well as enumerate order IDs and	8.2	More Details

	obtain valid order keys via GET requests, exposing customer order PII including names, addresses, and purchased products.		
CVE-2025-37168	Arbitrary file deletion vulnerability have been identified in a system function of mobility conductors running AOS-8 operating system. Successful exploitation of this vulnerability could allow an unauthenticated remote malicious actor to delete arbitrary files within the affected system and potentially result in denial-of-service conditions on affected devices.	8.2	More Details
CVE-2026-22817	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.11.4, there is a flaw in Hono’s JWK/JWKS JWT verification middleware allowed the JWT header’s alg value to influence signature verification when the selected JWK did not explicitly specify an algorithm. This could enable JWT algorithm confusion and, in certain configurations, allow forged tokens to be accepted. As part of this fix, the JWT middleware now requires the alg option to be explicitly specified. This prevents algorithm confusion by ensuring that the verification algorithm is not derived from untrusted JWT header values. This vulnerability is fixed in 4.11.4.	8.2	More Details
CVE-2026-21884	React Router is a router for React. In @remix-run/react version prior to 2.17.3. and react-router 7.0.0 through 7.11.0, a XSS vulnerability exists in in React Router's <ScrollRestoration> API in Framework Mode when using the getKey/storageKey props during Server-Side Rendering which could allow arbitrary JavaScript execution during SSR if untrusted content is used to generate the keys. There is no impact if server-side rendering in Framework Mode is disabled, or if Declarative Mode (<BrowserRouter>) or Data Mode (createBrowserRouter/<RouterProvider>) is being used. This issue has been patched in @remix-run/react version 2.17.3 and react-router version 7.12.0.	8.2	More Details
CVE-2022-50895	Aero CMS 0.0.1 contains a SQL injection vulnerability in the author parameter that allows attackers to manipulate database queries. Attackers can exploit boolean-based, error-based, time-based, and UNION query techniques to extract sensitive database information and potentially compromise the system.	8.2	More Details
CVE-2022-50892	VIAVIWEB Wallpaper Admin 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating login credentials. Attackers can exploit the login page by injecting 'admin' or 1=1-- - payload to gain unauthorized access to the administrative interface.	8.2	More Details
CVE-2022-50805	Senayan Library Management System 9.0.0 contains a SQL injection vulnerability in the 'class' parameter that allows attackers to inject malicious SQL queries. Attackers can exploit the vulnerability by submitting crafted payloads to manipulate database queries and potentially extract sensitive information.	8.2	More Details
CVE-2019-25279	FaceSentry Access Control System 6.4.8 contains a cleartext password storage vulnerability that allows attackers to access unencrypted credentials in the device's SQLite database. Attackers can directly read sensitive login information stored in /faceGuard/database/FaceSentryWeb.sqlite without additional authentication.	8.2	More Details
CVE-2026-22818	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.11.4, there is a flaw in Hono’s JWK/JWKS JWT verification middleware allowed the algorithm specified in the JWT header to influence signature verification when the selected JWK did not explicitly define an algorithm. This could enable JWT algorithm confusion and, in certain configurations, allow forged tokens to be accepted. The JWK/JWKS JWT verification middleware has been updated to require an explicit allowlist of asymmetric algorithms when verifying tokens. The middleware no longer derives the verification algorithm from untrusted JWT header values. This vulnerability is fixed in 4.11.4.	8.2	More Details
CVE-2025-46067	An issue in Automai Director v.25.2.0 allows a remote attacker to escalate privileges and obtain sensitive information via a crafted js file	8.2	More Details
CVE-2026-21898	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, the Crypto_AOS_ProcessSecurity function reads memory without valid bounds checking when parsing AOS frame hashes. This issue has been patched in version 1.4.3.	8.2	More Details
CVE-2025-71063	Errands before 46.2.10 does not verify TLS certificates for CalDAV servers.	8.2	More Details
CVE-2025-67925	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in zozothemes Corpkit corpkit allows PHP Local File Inclusion.This issue affects Corpkit: from n/a through <= 2.0.	8.1	More Details
CVE-2025-67917	Missing Authorization vulnerability in shinetheme Traveler traveler allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Traveler: from n/a through <= 3.2.6.	8.1	More Details
CVE-2025-67919	Authorization Bypass Through User-Controlled Key vulnerability in WofficeIO Woffice Core woffice-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Woffice Core: from n/a through <= 5.4.30.	8.1	More Details

CVE-2025-68472	MindsDB is a platform for building artificial intelligence from enterprise data. Prior to version 25.11.1, an unauthenticated path traversal in the file upload API lets any caller read arbitrary files from the server filesystem and move them into MindsDB's storage, exposing sensitive data. The PUT handler in file.py directly joins user-controlled data into a filesystem path when the request body is JSON and source_type is not "url". Only multipart uploads and URL-sourced uploads receive sanitization; JSON uploads lack any call to clear_filename or equivalent checks. This vulnerability is fixed in 25.11.1.	8.1	More Details
CVE-2025-62235	Authentication Bypass by Spoofing vulnerability in Apache NimBLE. Receiving specially crafted Security Request could lead to removal of original bond and re-bond with impostor. This issue affects Apache NimBLE: through 1.8.0. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	8.1	More Details
CVE-2025-22715	Missing Authorization vulnerability in loopus WP Attractive Donations System - Easy Stripe & Paypal donations WP_AttractiveDonationsSystem allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Attractive Donations System - Easy Stripe & Paypal donations: from n/a through <= 1.25.	8.1	More Details
CVE-2025-67934	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Wellspring wellspring allows PHP Local File Inclusion.This issue affects Wellspring: from n/a through < 2.8.	8.1	More Details
CVE-2026-0891	Memory safety bugs present in Firefox ESR 140.6, Thunderbird ESR 140.6, Firefox 146 and Thunderbird 146. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	8.1	More Details
CVE-2026-0506	Due to a Missing Authorization Check vulnerability in Application Server ABAP and ABAP Platform, an authenticated attacker could misuse an RFC function to execute form routines (FORMs) in the ABAP system. Successful exploitation could allow the attacker to write or modify data accessible via FORMs and invoke system functionality exposed via FORMs, resulting in a high impact on integrity and availability, while confidentiality remains unaffected.	8.1	More Details
CVE-2025-69080	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in JanStudio Gecko allows PHP Local File Inclusion.This issue affects Gecko: from n/a through 1.9.8.	8.1	More Details
CVE-2025-67089	A command injection vulnerability exists in the GL-iNet GL-AXT1800 router firmware v4.6.8. The vulnerability is present in the `plugins.install_package` RPC method, which fails to properly sanitize user input in package names. Authenticated attackers can exploit this to execute arbitrary commands with root privileges	8.1	More Details
CVE-2025-25249	A heap-based buffer overflow vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiOS 6.4.0 through 6.4.16, FortiSASE 25.2.b, FortiSASE 25.1.a.2, FortiSwitchManager 7.2.0 through 7.2.6, FortiSwitchManager 7.0.0 through 7.0.5 allows attacker to execute unauthorized code or commands via specially crafted packets	8.1	More Details
CVE-2026-0877	Mitigation bypass in the DOM: Security component. This vulnerability affects Firefox < 147, Firefox ESR < 115.32, and Firefox ESR < 140.7.	8.1	More Details
CVE-2025-11669	Zohocorp ManageEngine PAM360 versions before 8202; Password Manager Pro versions before 13221; Access Manager Plus versions prior to 4401 are vulnerable to an authorization issue in the initiate remote session functionality.	8.1	More Details
CVE-2026-20856	Improper input validation in Windows Server Update Service allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-22594	Ghost is a Node.js content management system. In versions 5.105.0 through 5.130.5 and 6.0.0 through 6.10.3, a vulnerability in Ghost's 2FA mechanism allows staff users to skip email 2FA. This issue has been patched in versions 5.130.6 and 6.11.0.	8.1	More Details
CVE-2026-22595	Ghost is a Node.js content management system. In versions 5.121.0 through 5.130.5 and 6.0.0 through 6.10.3, a vulnerability in Ghost's handling of Staff Token authentication allowed certain endpoints to be accessed that were only intended to be accessible via Staff Session authentication. External systems that have been authenticated via Staff Tokens for Admin/Owner-role users would have had access to these endpoints. This issue has been patched in versions 5.130.6 and 6.11.0.	8.1	More Details
CVE-2026-22687	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.5, after WeKnora enables the Agent service, it allows users to call the database query tool. Due to insufficient backend validation, an attacker can use prompt-based bypass techniques to evade query restrictions and obtain sensitive information from the target server and database. This issue has been patched in version 0.2.5.	8.1	More Details

CVE-2026-0511	SAP Fiori App Intercompany Balance Reconciliation does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has high impact on confidentiality and integrity of the application ,availability is not impacted.	8.1	More Details
CVE-2025-67935	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Optimize optimizewp allows PHP Local File Inclusion.This issue affects Optimize: from n/a through < 2.4.	8.1	More Details
CVE-2025-68493	Missing XML Validation vulnerability in Apache Struts, Apache Struts. This issue affects Apache Struts: from 2.0.0 before 2.2.1; Apache Struts: from 2.2.1 through 6.1.0. Users are recommended to upgrade to version 6.1.1, which fixes the issue.	8.1	More Details
CVE-2025-69081	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeREX Group Hope charity-is-hope allows PHP Local File Inclusion.This issue affects Hope: from n/a through 3.0.0.	8.1	More Details
CVE-2025-67937	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Hendon hendon allows PHP Local File Inclusion.This issue affects Hendon: from n/a through < 1.7.	8.1	More Details
CVE-2025-67936	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Curly curly allows PHP Local File Inclusion.This issue affects Curly: from n/a through < 3.3.	8.1	More Details
CVE-2026-22804	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 1.7.0 to 1.9.0, Stored Cross-Site Scripting (XSS) vulnerability exists in the Termix File Manager component. The application fails to sanitize SVG file content before rendering it. This allows an attacker who has compromised a managed SSH server to plant a malicious file, which, when previewed by the Termix user, executes arbitrary JavaScript in the context of the application. The vulnerability is located in src/ui/desktop/apps/file-manager/components/FileViewer.tsx. This vulnerability is fixed in 1.10.0.	8.0	More Details
CVE-2026-22704	HAX CMS helps manage microsite universe with PHP or NodeJs backends. In versions 11.0.6 to before 25.0.0, HAX CMS is vulnerable to stored XSS, which could lead to account takeover. This issue has been patched in version 25.0.0.	8.0	More Details
CVE-2025-13761	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed an unauthenticated user to execute arbitrary code in the context of an authenticated user's browser by convincing the legitimate user to visit a specially crafted webpage.	8.0	More Details
CVE-2026-0878	Sandbox escape due to incorrect boundary conditions in the Graphics: CanvasWebGL component. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	8.0	More Details
CVE-2026-22029	React Router is a router for React. In @remix-run/router version prior to 1.23.2. and react-router 7.0.0 through 7.11.0, React Router (and Remix v1/v2) SPA open navigation redirects originating from loaders or actions in Framework Mode, Data Mode, or the unstable RSC modes can result in unsafe URLs causing unintended javascript execution on the client. This is only an issue if you are creating redirect paths from untrusted content or via an open redirect. There is no impact if Declarative Mode (<BrowserRouter>) is being used. This issue has been patched in @remix-run/router version 1.23.2 and react-router version 7.12.0.	8.0	More Details
CVE-2025-66620	An unused webshell in MicroServer allows unlimited login attempts, with sudo rights on certain files and directories. An attacker with admin access to MicroServer can gain limited shell access, enabling persistence through reverse shells, and the ability to modify or remove data stored in the file system.	8.0	More Details
CVE-2026-20931	External control of file name or path in Windows Telephony Service allows an authorized attacker to elevate privileges over an adjacent network.	8.0	More Details
CVE-2026-20826	Concurrent execution using shared resource with improper synchronization ('race condition') in Tablet Windows User Interface (TWINUI) Subsystem allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20840	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	7.8	More Details
CVE-2026-20822	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20809	Time-of-check time-of-use (toctou) race condition in Windows Kernel Memory allows an authorized attacker to elevate privileges locally.	7.8	More Details

CVE-2026-20810	Free of memory not on the heap in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20843	Improper access control in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20820	Heap-based buffer overflow in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21678	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to heap-buffer-overflow vulnerability in IccTagXml(). This issue has been patched in version 2.3.1.2.	7.8	More Details
CVE-2026-20837	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-20817	Improper handling of insufficient permissions or privileges in Windows Error Reporting allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20811	Access of resource using incompatible type ('type confusion') in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20832	Windows Remote Procedure Call Interface Definition Language (IDL) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2026-20816	Time-of-check time-of-use (toctou) race condition in Windows Installer allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20831	Time-of-check time-of-use (toctou) race condition in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20857	Untrusted pointer dereference in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21276	InDesign Desktop versions 21.0, 19.5.5 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-20858	Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-47343	Memory corruption while processing a video session to set video parameters.	7.8	More Details
CVE-2025-47339	Memory corruption while deinitializing a HDCP session.	7.8	More Details
CVE-2026-20949	Improper access control in Microsoft Office Excel allows an unauthorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-20950	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-20951	Improper input validation in Microsoft Office SharePoint allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code		More

2026-20955	locally.	7.8	Details
CVE-2026-20956	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-20957	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-21224	Stack-based buffer overflow in Azure Connected Machine Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21274	Dreamweaver Desktop versions 21.6 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could leverage this vulnerability to bypass security measures and execute unauthorized code. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21275	InDesign Desktop versions 21.0, 19.5.5 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21277	InDesign Desktop versions 21.0, 19.5.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-47348	Memory corruption while processing identity credential operations in the trusted application.	7.8	More Details
CVE-2026-21281	InCopy versions 21.0, 19.5.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21283	Bridge versions 15.1.2, 16.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21304	InDesign Desktop versions 21.0, 19.5.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-0830	Processing specially crafted workspace folder names could allow for arbitrary command injection in the Kiro GitLab Merge-Request helper in Kiro IDE before version 0.6.18 when opening maliciously crafted workspaces. To mitigate, users should update to the latest version.	7.8	More Details
CVE-2026-21287	Substance3D - Stager versions 3.1.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21305	Substance3D - Painter versions 11.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21306	Substance3D - Sampler versions 5.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21307	Substance3D - Designer versions 15.0.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-37186	A local privilege-escalation vulnerability has been discovered in the HPE Aruba Networking Virtual Intranet Access (VIA) client. Successful exploitation of this vulnerability could allow a local attacker to achieve arbitrary code execution with root privileges.	7.8	More Details
CVE-2026-21298	Substance3D - Modeler versions 1.22.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-	Substance3D - Modeler versions 1.22.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires	7.8	More

21299	user interaction in that a victim must open a malicious file.		Details
CVE-2025-55125	This vulnerability allows a Backup or Tape Operator to perform remote code execution (RCE) as root by creating a malicious backup configuration file.	7.8	More Details
CVE-2025-47346	Memory corruption while processing a secure logging command in the trusted application.	7.8	More Details
CVE-2026-20948	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-47356	Memory Corruption when multiple threads concurrently access and modify shared resources.	7.8	More Details
CVE-2026-20920	Use after free in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20859	Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20860	Access of resource using incompatible type ('type confusion') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20861	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20864	Heap-based buffer overflow in Connected Devices Platform Service (Cdpsvc) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20865	Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20866	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20867	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20870	Use after free in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20871	Use after free in Desktop Windows Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20873	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20874	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20877	Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-47380	Memory corruption while preprocessing IOCTLs in sensors.	7.8	More Details

CVE-2026-20918	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20922	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	7.8	More Details
CVE-2026-20941	Improper link resolution before file access ('link following') in Host Process for Windows Tasks allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-47388	Memory corruption while passing pages to DSP with an unaligned starting address.	7.8	More Details
CVE-2025-47394	Memory corruption when copying overlapping buffers during memory operations due to incorrect offset calculations.	7.8	More Details
CVE-2026-20946	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-47396	Memory corruption occurs when a secure application is launched on a device with insufficient memory.	7.8	More Details
CVE-2025-47393	Memory corruption when accessing resources in kernel driver.	7.8	More Details
CVE-2026-20940	Heap-based buffer overflow in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20938	Untrusted pointer dereference in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20924	Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20923	Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-20804	Incorrect privilege assignment in Windows Hello allows an unauthorized attacker to perform tampering locally.	7.7	More Details
CVE-2025-14804	The Frontend File Manager Plugin WordPress plugin before 23.5 did not validate a path parameter and ownership of the file, allowing any authenticated users, such as subscribers to delete arbitrary files on the server	7.7	More Details
CVE-2026-20852	Incorrect privilege assignment in Windows Hello allows an unauthorized attacker to perform tampering locally.	7.7	More Details
CVE-2026-22035	Greenshot is an open source Windows screenshot utility. Versions 1.3.310 and below arvulnerable to OS Command Injection through unsanitized filename processing. The FormatArguments method in ExternalCommandDestination.cs:269 uses string.Format() to insert user-controlled filenames directly into shell commands without sanitization, allowing attackers to execute arbitrary commands by crafting malicious filenames containing shell metacharacters. This issue is fixed in version 1.3.311.	7.7	More Details
CVE-2025-59057	React Router is a router for React. In @remix-run/react versions 1.15.0 through 2.17.0. and react-router versions 7.0.0 through 7.8.2, a XSS vulnerability exists in in React Router's meta()/<Meta> APIs in Framework Mode when generating script:ld+json tags which could allow arbitrary JavaScript execution during SSR if untrusted content is used to generate the tag. There is no impact if the application is being used in Declarative Mode (<BrowserRouter>) or Data Mode (createBrowserRouter/<RouterProvider>). This issue has been patched in @remix-run/react version 2.17.1 and react-router version 7.9.0.	7.6	More Details
	A flaw was found in GNU Wget2. This vulnerability, a stack-based buffer overflow, occurs in the filename		

CVE-2025-69195	sanitization logic when processing attacker-controlled URL paths, particularly when filename restriction options are active. A remote attacker can exploit this by providing a specially crafted URL, which, upon user interaction with wget2, can lead to memory corruption. This can cause the application to crash and potentially allow for further malicious activities.	7.6	More Details
CVE-2026-22230	OPEXUS eCASE Audit allows an authenticated attacker to modify client-side JavaScript or craft HTTP requests to access functions or buttons that have been disabled or blocked by an administrator. Fixed in eCASE Platform 11.14.1.0.	7.6	More Details
CVE-2017-20213	FLIR Thermal Camera F/FC/PT/D Stream firmware version 8.0.0.64 contains an unauthenticated vulnerability that allows remote attackers to access live camera streams without credentials. Attackers can exploit the vulnerability to view unauthorized thermal camera video feeds across multiple camera series without requiring any authentication.	7.5	More Details
CVE-2025-67931	Insertion of Sensitive Information Into Sent Data vulnerability in AITpro BulletProof Security bulletproof-security allows Retrieve Embedded Sensitive Data.This issue affects BulletProof Security: from n/a through <= 6.9.	7.5	More Details
CVE-2026-20965	Improper verification of cryptographic signature in Windows Admin Center allows an authorized attacker to elevate privileges locally.	7.5	More Details
CVE-2026-22589	Spree is an open source e-commerce solution built with Ruby on Rails. Prior to versions 4.10.2, 5.0.7, 5.1.9, and 5.2.5, an Unauthenticated Insecure Direct Object Reference (IDOR) vulnerability was identified that allows an unauthenticated attacker to access guest address information without supplying valid credentials or session cookies. This issue has been patched in versions 4.10.2, 5.0.7, 5.1.9, and 5.2.5.	7.5	More Details
CVE-2026-22699	RustCrypto: Elliptic Curves is general purpose Elliptic Curve Cryptography (ECC) support, including types and traits for representing various elliptic curve forms, scalars, points, and public/secret keys composed thereof. In versions 0.14.0-pre.0 and 0.14.0-rc.0, a denial-of-service vulnerability exists in the SM2 PKE decryption path where an invalid elliptic-curve point (C1) is decoded and the resulting value is unwrapped without checking. Specifically, AffinePoint::from_encoded_point(&encoded_c1) may return a None/CtOption::None when the supplied coordinates are syntactically valid but do not lie on the SM2 curve. The calling code previously used .unwrap(), causing a panic when presented with such input. This issue has been patched via commit 085b7be.	7.5	More Details
CVE-2026-22700	RustCrypto: Elliptic Curves is general purpose Elliptic Curve Cryptography (ECC) support, including types and traits for representing various elliptic curve forms, scalars, points, and public/secret keys composed thereof. In versions 0.14.0-pre.0 and 0.14.0-rc.0, a denial-of-service vulnerability exists in the SM2 public-key encryption (PKE) implementation: the decrypt() path performs unchecked slice::split_at operations on input buffers derived from untrusted ciphertext. An attacker can submit short/undersized ciphertext or carefully-crafted DER-encoded structures to trigger bounds-check panics (Rust unwinding) which crash the calling thread or process. This issue has been patched via commit e60e991.	7.5	More Details
CVE-2026-20934	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2026-20929	Improper access control in Windows HTTP.sys allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2017-20214	FLIR Thermal Camera F/FC/PT/D firmware version 8.0.0.64 contains hard-coded SSH credentials that cannot be changed through normal camera operations. Attackers can leverage these persistent, unmodifiable credentials to gain unauthorized remote access to the thermal camera system.	7.5	More Details
CVE-2026-22777	ComfyUI-Manager is an extension designed to enhance the usability of ComfyUI. Prior to versions 3.39.2 and 4.0.5, an attacker can inject special characters into HTTP query parameters to add arbitrary configuration values to the config.ini file. This can lead to security setting tampering or modification of application behavior. This issue has been patched in versions 3.39.2 and 4.0.5.	7.5	More Details
CVE-2026-20921	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2026-22697	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, CryptoLib's KMC crypto service integration is vulnerable to a heap buffer overflow when decoding Base64-encoded ciphertext/cleartext fields returned by the KMC service. The decode destination buffer is sized using an expected output length (len_data_out), but the Base64 decoder writes output based on the actual Base64 input length and does not enforce any destination size limit. An oversized Base64 string in the KMC JSON response can cause out-of-bounds writes on the heap,	7.5	More Details

	resulting in process crash and potentially code execution under certain conditions. This issue has been patched in version 1.4.3.		
CVE-2026-20919	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2025-52435	J2EE Misconfiguration: Data Transmission Without Encryption vulnerability in Apache NimBLE. Improper handling of Pause Encryption procedure on Link Layer results in a previously encrypted connection being left in un-encrypted state allowing an eavesdropper to observe the remainder of the exchange. This issue affects Apache NimBLE: through <= 1.8.0. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	7.5	More Details
CVE-2025-53477	NULL Pointer Dereference vulnerability in Apache Nimble. Missing validation of HCI connection complete or HCI command TX buffer could lead to NULL pointer dereference. This issue requires disabled asserts and broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.8.0. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	7.5	More Details
CVE-2026-20875	Null pointer dereference in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2025-67914	Path Traversal: '.../...//' vulnerability in beeteam368 VidMov vidmov allows Path Traversal.This issue affects VidMov: from n/a through <= 2.3.8.	7.5	More Details
CVE-2025-65805	OpenAirInterface CN5G AMF<=v2.1.9 has a buffer overflow vulnerability in processing NAS messages. Unauthorized remote attackers can launch a denial-of-service attack and potentially execute malicious code by accessing port N1 and sending an imsi string longer than 1000 to AMF.	7.5	More Details
CVE-2025-66786	OpenAirInterface CN5G AMF<=v2.0.1 There is a logical error when processing JSON format requests. Unauthorized remote attackers can send malicious JSON data to AMF's SBI interface to launch a denial-of-service attack.	7.5	More Details
CVE-2025-67364	fast-filesystem-mcp version 3.4.0 contains a critical path traversal vulnerability in its file operation tools including fast_read_file. This vulnerability arises from improper path validation that fails to resolve symbolic links to their actual physical paths. The safePath and isPathAllowed functions use path.resolve() which does not handle symlinks, allowing attackers to bypass directory access restrictions by creating symlinks within allowed directories that point to restricted system paths. When these symlinks are accessed through valid path references, the validation checks are circumvented, enabling access to unauthorized files.	7.5	More Details
CVE-2026-21226	Deserialization of untrusted data in Azure Core shared client library for Python allows an authorized attacker to execute code over a network.	7.5	More Details
CVE-2025-69259	A message unchecked NULL return value vulnerability in Trend Micro Apex Central could allow a remote attacker to create a denial-of-service condition on affected installations. Please note: authentication is not required in order to exploit this vulnerability..	7.5	More Details
CVE-2026-20854	Use after free in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to execute code over a network.	7.5	More Details
CVE-2025-13493	The Latest Registered Users plugin for WordPress is vulnerable to unauthorized user data export in all versions up to, and including, 1.4. This is due to missing authorization and nonce validation in the rnd_handle_form_submit function hooked to both admin_post_my_simple_form and admin_post_nopriv_my_simple_form actions. This makes it possible for unauthenticated attackers to export complete user details (excluding passwords and sensitive tokens) in CSV format via the 'action' parameter.	7.5	More Details
CVE-2026-22235	OPEXUS eComplaint before version 9.0.45.0 allows an attacker to visit the the 'DocumentOpen.aspx' endpoint, iterate through predictable values of 'chargeNumber', and download any uploaded files.	7.5	More Details
CVE-2025-65518	Plesk Obsidian versions 8.0.1 through 18.0.73 are vulnerable to a Denial of Service (DoS) condition. The vulnerability exists in the get_password.php endpoint, where a crafted request containing a malicious payload can cause the affected web interface to continuously reload, rendering the service unavailable to legitimate users. An attacker can exploit this issue remotely without authentication, resulting in a persistent availability impact on the affected Plesk Obsidian instance.	7.5	More Details
CVE-2023-54337	Sysax Multi Server 6.95 contains a denial of service vulnerability in the administrative password field that allows attackers to crash the application. Attackers can overwrite the password field with 800 bytes of repeated characters to trigger an application crash and disrupt server functionality.	7.5	More Details

CVE-2025-11877	The User Activity Log plugin is vulnerable to a limited options update in versions up to, and including, 2.2. The failed-login handler 'ual_shook_wp_login_failed' lacks a capability check and writes failed usernames directly into update_option() calls. This makes it possible for unauthenticated attackers to push select site options from 0 to a non-zero value, allowing them to reopen registration or corrupt options like 'wp_user_roles', breaking wp-admin access.	7.5	More Details
CVE-2025-56424	An issue in Insiders Technologies GmbH e-invoice pro before release 1 Service Pack 2 allows a remote attacker to cause a denial of service via a crafted script	7.5	More Details
CVE-2025-50334	An issue in Technitium DNS Server v.13.5 allows a remote attacker to cause a denial of service via the rate-limiting component	7.5	More Details
CVE-2025-15464	Exported Activity allows external applications to gain application context and directly launch Gmail with inbox access, bypassing security controls.	7.5	More Details
CVE-2022-50932	Kyocera Command Center RX ECOSYS M2035dn contains a directory traversal vulnerability that allows unauthenticated attackers to read sensitive system files by manipulating file paths under the /js/ path. Attackers can exploit the issue by sending requests like /js/../../../.../etc/passwd%00.jpg (null-byte appended traversal) to access critical files such as /etc/passwd and /etc/shadow.	7.5	More Details
CVE-2025-13801	The Yoco Payments plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 3.8.8 via the file parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2025-69260	A message out-of-bounds read vulnerability in Trend Micro Apex Central could allow a remote attacker to create a denial-of-service condition on affected installations. Please note: authentication is not required in order to exploit this vulnerability.	7.5	More Details
CVE-2022-50910	Beehive Forum 1.5.2 contains a host header injection vulnerability in the forgot password functionality that allows attackers to manipulate password reset requests. Attackers can inject a malicious host header to intercept password reset tokens and change victim account passwords without direct authentication.	7.5	More Details
CVE-2025-14070	The Reviewify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'send_test_email' AJAX action in all versions up to, and including, 1.0.6. This makes it possible for authenticated attackers, with Contributor-level access and above, to create arbitrary WooCommerce discount coupons, potentially causing financial loss to the store.	7.5	More Details
CVE-2022-50890	Owlfiles File Manager 12.0.1 contains a path traversal vulnerability in its built-in HTTP server that allows attackers to access system directories. Attackers can exploit the vulnerability by crafting GET requests with directory traversal sequences to access restricted system directories on the device.	7.5	More Details
CVE-2021-47751	CuteEditor for PHP (now referred to as Rich Text Editor) 6.6 contains a directory traversal vulnerability in the browse template feature that allows attackers to write files to arbitrary web root directories. Attackers can exploit the ServerMapPath() function by renaming uploaded HTML files using directory traversal sequences to write files outside the intended template directory.	7.5	More Details
CVE-2025-64092	This vulnerability allows unauthenticated attackers to inject an SQL request into GET request parameters and directly query the underlying database.	7.5	More Details
CVE-2025-56225	fluidsynth-2.4.6 and earlier versions is vulnerable to Null pointer dereference in fluid_synth_monopoly.c, that can be triggered when loading an invalid midi file.	7.5	More Details
CVE-2025-67133	An issue in Hero Motocorp Vida V1 Pro 2.0.7 allows a local attacker to cause a denial of service via the BLE component	7.5	More Details
CVE-2025-66744	In Yonyou YonBIP v3 and before, the LoginWithV8 interface in the series data application service system is vulnerable to path traversal, allowing unauthorized access to sensitive information within the system	7.5	More Details
CVE-2025-67366	@sylphxltd/filesystem-mcp v0.5.8 is an MCP server that provides file content reading functionality. Version 0.5.8 of filesystem-mcp contains a critical path traversal vulnerability in its "read_content" tool. This vulnerability arises from improper symlink handling in the path validation mechanism: the resolvePath function checks path validity before resolving symlinks, while fs.readFile resolves symlinks automatically during file access. This allows attackers to bypass directory restrictions by leveraging symlinks within the allowed directory that point to external files, enabling unauthorized access to files outside the intended operational scope.	7.5	More Details

CVE-2026-20926	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2025-13457	The WooCommerce Square plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.1.1 via the get_token_by_id function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to expose arbitrary Square "ccof" (credit card on file) values and leverage this value to potentially make fraudulent charges on the target site.	7.5	More Details
CVE-2026-0669	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Wikimedia Foundation MediaWiki - CSS extension allows Path Traversal.This issue affects MediaWiki - CSS extension: 1.44, 1.43, 1.39.	7.5	More Details
CVE-2025-37166	A vulnerability affecting HPE Networking Instant On Access Points has been identified where a device processing a specially crafted packet could enter a non-responsive state, in some cases requiring a hard reset to re-establish services. A malicious actor could leverage this vulnerability to conduct a Denial-of-Service attack on a target network.	7.5	More Details
CVE-2026-22521	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in G5Theme Handmade Framework allows PHP Local File Inclusion.This issue affects Handmade Framework: from n/a through 3.9.	7.5	More Details
CVE-2026-21868	Flag Forge is a Capture The Flag (CTF) platform. Versions 2.3.2 and below have a Regular Expression Denial of Service (ReDoS) vulnerability in the user profile API endpoint (/api/user/[username]). The application constructs a regular expression dynamically using unescaped user input (the username parameter). An attacker can exploit this by sending a specially crafted username containing regex meta-characters (e.g., deeply nested groups or quantifiers), causing the MongoDB regex engine to consume excessive CPU resources. This can lead to Denial of Service for other users. The issue is fixed in version 2.3.3. To workaround this issue, implement a Web Application Firewall (WAF) rule to block requests containing regex meta-characters in the URL path.	7.5	More Details
CVE-2026-22190	Panda3D versions up to and including 1.10.16 egg-mkfont contains an uncontrolled format string vulnerability. The -gp (glyph pattern) command-line option is used directly as the format string for sprintf() with only a single argument supplied. If an attacker provides additional format specifiers, egg-mkfont may read unintended stack values and write the formatted output into generated .egg and .png files, resulting in disclosure of stack-resident memory and pointer values.	7.5	More Details
CVE-2025-37165	A vulnerability in the router mode configuration of HPE Instant On Access Points exposed certain network configuration details to unintended interfaces. A malicious actor could gain knowledge of internal network configuration details through inspecting impacted packets.	7.5	More Details
CVE-2025-13151	Stack-based buffer overflow in libtasn1 version: v4.20.0. The function fails to validate the size of input data resulting in a buffer overflow in asn1_expend_octet_string.	7.5	More Details
CVE-2025-40944	A vulnerability has been identified in SIMATIC ET 200AL IM 157-1 PN (6ES7157-1AB00-0AB0) (All versions), SIMATIC ET 200MP IM 155-5 PN HF (6ES7155-5AA00-0AC0) (All versions >= V4.2.0), SIMATIC ET 200SP IM 155-6 MF HF (6ES7155-6MU00-0CN0) (All versions), SIMATIC ET 200SP IM 155-6 PN HA (incl. SIPLUS variants) (All versions < V1.3), SIMATIC ET 200SP IM 155-6 PN R1 (6ES7155-6AU00-0HM0) (All versions < V6.0.1), SIMATIC ET 200SP IM 155-6 PN/2 HF (6ES7155-6AU01-0CN0) (All versions >= V4.2.0), SIMATIC ET 200SP IM 155-6 PN/3 HF (6ES7155-6AU30-0CN0) (All versions < V4.2.2), SIMATIC PN/MF Coupler (6ES7158-3MU10-0XA0) (All versions), SIMATIC PN/PN Coupler (6ES7158-3AD10-0XA0) (All versions < V6.0.0), SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-2AC0) (All versions >= V4.2.0), SIPLUS ET 200MP IM 155-5 PN HF (6AG1155-5AA00-7AC0) (All versions >= V4.2.0), SIPLUS ET 200MP IM 155-5 PN HF T1 RAIL (6AG2155-5AA00-1AC0) (All versions >= V4.2.0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-2CN0) (All versions >= V4.2.0), SIPLUS ET 200SP IM 155-6 PN HF (6AG1155-6AU01-7CN0) (All versions >= V4.2.0), SIPLUS ET 200SP IM 155-6 PN HF T1 RAIL (6AG2155-6AU01-1CN0) (All versions >= V4.2.0), SIPLUS ET 200SP IM 155-6 PN HF TX RAIL (6AG2155-6AU01-4CN0) (All versions >= V4.2.0), SIPLUS NET PN/PN Coupler (6AG2158-3AD10-4XA0) (All versions < V6.0.0). Affected devices do not properly handle S7 protocol session disconnect requests. When receiving a valid S7 protocol Disconnect Request (COTP DR TPDU) on TCP port 102, the devices enter an improper session state. This could allow an attacker to cause the device to become unresponsive, leading to a denial-of-service condition that requires a power cycle to restore normal operation.	7.5	More Details
CVE-2019-25291	INIM Electronics Smartliving SmartLAN/G/SI <=6.x contains hard-coded credentials in its Linux distribution image that cannot be changed through normal device operations. Attackers can exploit these persistent credentials to log in and gain unauthorized system access across multiple SmartLiving device models.	7.5	More Details
CVE-2025-69263	pnpm is a package manager. Versions 10.26.2 and below store HTTP tarball dependencies (and git-hosted tarballs) in the lockfile without integrity hashes. This allows the remote server to serve different content on each install, even when a lockfile is committed. An attacker who publishes a package with an HTTP tarball dependency can serve different code to different users or CI/CD environments. The attack requires the victim to install a package that has an HTTP/git tarball in its dependency tree. The victim's lockfile provides no	7.5	More Details

	protection. This issue is fixed in version 10.26.0.		
CVE-2019-25278	FaceSentry Access Control System 6.4.8 contains a cleartext transmission vulnerability that allows remote attackers to intercept authentication credentials. Attackers can perform man-in-the-middle attacks to capture HTTP cookie authentication information during network communication.	7.5	More Details
CVE-2025-46685	Dell SupportAssist OS Recovery, versions prior to 5.5.15.1, contain a Creation of Temporary File With Insecure Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.5	More Details
CVE-2025-71023	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow in the mac2 parameter of the fromAdvSetMacMtuWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2026-20848	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2026-20849	Reliance on untrusted inputs in a security decision in Windows Kerberos allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2025-69262	pnpm is a package manager. Versions 6.25.0 through 10.26.2 have a Command Injection vulnerability when using environment variable substitution in .npmrc configuration files with tokenHelper settings. An attacker who can control environment variables during pnpm operations could achieve Remote Code Execution (RCE) in build environments. This issue is fixed in version 10.27.0.	7.5	More Details
CVE-2026-0889	Denial-of-service in the DOM: Service Workers component. This vulnerability affects Firefox < 147.	7.5	More Details
CVE-2026-0386	Improper access control in Windows Deployment Services allows an unauthorized attacker to execute code over an adjacent network.	7.5	More Details
CVE-2026-20844	Use after free in Windows Clipboard Server allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2026-20853	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows WalletService allows an unauthorized attacker to elevate privileges locally.	7.4	More Details
CVE-2026-0643	A flaw has been found in projectworlds House Rental and Property Listing 1.0. Impacted is an unknown function of the file /app/register.php?action=reg of the component Signup. This manipulation of the argument image causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used.	7.3	More Details
CVE-2026-21897	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, the Crypto_Config_Add_Gvcid_Managed_Parameters function only checks whether gvcid_counter > GVCID_MAN_PARAM_SIZE. As a result, it allows up to the 251st entry, which causes a write past the end of the array, overwriting gvcid_counter located immediately after gvcid_managed_parameters_array[250]. This leads to an out-of-bounds write, and the overwritten gvcid_counter may become an arbitrary value, potentially affecting the parameter lookup/registration logic that relies on it. This issue has been patched in version 1.4.3.	7.3	More Details
CVE-2026-0851	A vulnerability was identified in code-projects Online Music Site 1.0. The affected element is an unknown function of the file /Administrator/PHP/AdminAddUser.php. The manipulation of the argument txtusername 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-2025-15503	A security flaw has been discovered in Sangfor Operation and Maintenance Management System up to 3.0.8. The impacted element is an unknown function of the file /fort/trust/version/common/common.jsp. Performing a manipulation of the argument File results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-0852	A security flaw has been discovered in code-projects Online Music Site 1.0. The impacted element is an unknown function of the file /Administrator/PHP/AdminUpdateUser.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details

CVE-2026-0821	A vulnerability was determined in quickjs-ng quickjs up to 0.11.0. This vulnerability affects the function js_typed_array_constructor of the file quickjs.c. Executing a manipulation can lead to heap-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called c5d80831e51e48a83eab16ea867be87f091783c5. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2026-0700	A vulnerability was determined in code-projects Intern Membership Management System 1.0. Affected is an unknown function of the file /intern/admin/check_admin.php. Executing a manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-15502	A vulnerability was identified in Sangfor Operation and Maintenance Management System up to 3.0.8. The affected element is the function SessionController of the file /isomp-protocol/protocol/session. Such manipulation of the argument Hostname 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.	7.3	More Details
CVE-2025-14937	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'acff' parameter in the 'frontend_admin/forms/update_field' AJAX action in all versions up to, and including, 3.28.23 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-37171	Authenticated command injection vulnerabilities exist in the web-based management interface of mobility conductors running AOS-8 operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2025-37172	Authenticated command injection vulnerabilities exist in the web-based management interface of mobility conductors running AOS-8 operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2025-37173	An improper input handling vulnerability exists in the web-based management interface of mobility conductors running either AOS-10 or AOS-8 operating systems. Successful exploitation could allow an authenticated malicious actor with valid credentials to trigger unintended behavior on the affected system.	7.2	More Details
CVE-2025-37174	Authenticated arbitrary file write vulnerability exists in the web-based management interface of mobility conductors running either AOS-10 or AOS-8 operating systems. Successful exploitation could allow an authenticated malicious actor to create or modify arbitrary files and execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2025-37175	Arbitrary file upload vulnerability exists in the web-based management interface of mobility conductors running either AOS-10 or AOS-8 operating systems. Successful exploitation could allow an authenticated malicious actor to upload arbitrary files as a privilege user and execute arbitrary commands on the underlying operating system.	7.2	More Details
CVE-2022-50908	Mailhog 1.0.1 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts through email attachments. Attackers can send crafted emails with XSS payloads to execute arbitrary API calls, including message deletion and browser manipulation.	7.2	More Details
CVE-2025-59922	An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] vulnerability in Fortinet FortiClientEMS 7.4.3 through 7.4.4, FortiClientEMS 7.4.0 through 7.4.1, FortiClientEMS 7.2.0 through 7.2.10, FortiClientEMS 7.0 all versions may allow an authenticated attacker with at least read-only admin permission to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests.	7.2	More Details
CVE-2025-14657	The Eventin – Event Manager, Events Calendar, Event Tickets and Registrations plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'post_settings' function in all versions up to, and including, 4.0.51. This makes it possible for unauthenticated attackers to modify plugin settings. Furthermore, due to insufficient input sanitization and output escaping on the 'etn_primary_color' setting, this enables unauthenticated attackers to inject arbitrary web scripts that will execute whenever a user accesses a page where Eventin styles are loaded.	7.2	More Details
CVE-2025-37169	A stack overflow vulnerability exists in the AOS-10 web-based management interface of a Mobility Gateway. Successful exploitation could allow an authenticated malicious actor to execute arbitrary code as a privileged user on the underlying operating system.	7.2	More Details
CVE-2025-15057	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `fh` (fingerprint) parameter in all versions up to, and including, 5.3.3. This is due to insufficient input sanitization and output escaping on the fingerprint value stored in the database. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator views the Real-time Access Log report.	7.2	More Details
	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'notes' and		

CVE-2025-15055	'resource' parameters in all versions up to, and including, 5.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the Recent Custom Events report.	7.2	More Details
CVE-2025-14436	The Brevo for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘user_connection_id’ parameter in all versions up to, and including, 4.0.49 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2022-50937	Ametys CMS v4.4.1 contains a persistent cross-site scripting vulnerability in the link directory's input fields for external links. Attackers can inject malicious script code in link text and descriptions to execute persistent attacks that compromise user sessions and manipulate application modules.	7.2	More Details
CVE-2022-50939	e107 CMS version 3.2.1 contains a critical file upload vulnerability that allows authenticated administrators to override arbitrary server files through path traversal. The vulnerability exists in the Media Manager's remote URL upload functionality (image.php) where the upload_caption parameter is not properly sanitized. An attacker with administrative privileges can use directory traversal sequences (../../../) in the upload_caption field to overwrite critical system files outside the intended upload directory. This can lead to complete compromise of the web application by overwriting configuration files, executable scripts, or other critical system components. The vulnerability was discovered by Hubert Wojciechowski and affects the image.php component in the admin interface.	7.2	More Details
CVE-2025-37170	Authenticated command injection vulnerabilities exist in the web-based management interface of mobility conductors running AOS-8 operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2026-20803	Missing authentication for critical function in SQL Server allows an authorized attacker to elevate privileges over a network.	7.2	More Details
CVE-2026-21873	NiceGUI is a Python-based UI framework. From versions 2.22.0 to 3.4.1, an unsafe implementation in the pushstate event listener used by ui.sub_pages allows an attacker to manipulate the fragment identifier of the URL, which they can do despite being cross-site, using an iframe. This issue has been patched in version 3.5.0.	7.2	More Details
CVE-2025-15472	A flaw has been found in TRENDnet TEW-811DRU 1.0.2.0. This affects the function setDeviceURL of the file uapply.cgi of the component httpd . This manipulation of the argument DeviceURL causes os command injection. The attack can 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.	7.2	More Details
CVE-2026-21856	The Tarkov Data Manager is a tool to manage the Tarkov item data. Prior to commit 9bdb3a75a98a7047b6d70144eb1da1655d6992a8, a time based blind SQL injection vulnerability in the webhook edit and scanner api endpoints that allow an authenticated attacker to execute arbitrary SQL queries against the MySQL database. Commit 9bdb3a75a98a7047b6d70144eb1da1655d6992a8 contains a patch.	7.2	More Details
CVE-2025-46494	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themesgrove WidgetKit Pro allows Reflected XSS.This issue affects WidgetKit Pro: from n/a through 1.13.1.	7.1	More Details
CVE-2026-21681	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Undefined Behavior runtime error. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	7.1	More Details
CVE-2025-68874	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shahjada Visitor Stats Widget visitor-stats-widget allows Reflected XSS.This issue affects Visitor Stats Widget: from n/a through <= 1.5.0.	7.1	More Details
CVE-2025-68887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CMSJunkie - WordPress Business Directory Plugins WP-BusinessDirectory wp-businessdirectory allows Reflected XSS.This issue affects WP-BusinessDirectory: from n/a through <= 3.1.5.	7.1	More Details
CVE-2026-21686	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have Undefined Behavior in `CIccTagLutAtoB::Validate()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	7.1	More Details
CVE-2026-21685	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have Undefined Behavior in `CIccTagLut16::Read()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	7.1	More Details

CVE-2026-21684	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have Undefined Behavior in `CIccTagSpectralViewingConditions()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	7.1	More Details
CVE-2025-68889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pinpoll Pinpoll pinpoll allows Reflected XSS.This issue affects Pinpoll: from n/a through <= 4.0.0.	7.1	More Details
CVE-2025-68873	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chloédigital PRIMER by chloédigital primer-by-chloedigital allows Reflected XSS.This issue affects PRIMER by chloédigital: from n/a through <= 1.0.25.	7.1	More Details
CVE-2025-69082	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Frenify Arlo arlo allows Reflected XSS.This issue affects Arlo: from n/a through 6.0.3.	7.1	More Details
CVE-2025-32300	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital zoom studio DZS Video Gallery allows Reflected XSS.This issue affects DZS Video Gallery: from n/a through 12.25.	7.1	More Details
CVE-2025-69220	LibreChat is a ChatGPT clone with additional features. Version 0.8.1-rc2 does not enforce proper access control for file uploads to an agents file context and file search. An authenticated attacker with access to the agent ID can change the behavior of arbitrary agents by uploading new files to the file context or file search, even if they have no permissions for this agent. This issue is fixed in version 0.8.2-rc2.	7.1	More Details
CVE-2025-31642	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dasinfomedia WPCHURCH allows Reflected XSS.This issue affects WPCHURCH: from n/a through 2.7.0.	7.1	More Details
CVE-2026-21687	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have Undefined Behavior in `CIccTagCurve::CIccTagCurve()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	7.1	More Details
CVE-2025-13772	GitLab has remediated an issue in GitLab EE affecting all versions from 18.4 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed an authenticated user to access and utilize AI model settings from unauthorized namespaces by manipulating namespace identifiers in API requests.	7.1	More Details
CVE-2025-14835	The WP Photo Album Plus plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘shortcode’ parameter in all versions up to, and including, 9.1.05.008 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	7.1	More Details
CVE-2026-20842	Use after free in Windows DWM allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-20830	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-20869	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Local Session Manager (LSM) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-21219	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2026-20943	Untrusted search path in Microsoft Office allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2026-21221	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-20808	Concurrent execution using shared resource with improper synchronization ('race condition') in Printer Association Object allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-			

2026-20836	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-20863	Double free in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-20814	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-20815	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-61547	Cross-Site Request Forgery (CSRF) is present on all functions in edu Business Solutions Print Shop Pro WebDesk version 18.34. The application does not implement proper CSRF tokens or other other protective measures, allowing a remote attacker to trick authenticated users into unknowingly executing unintended actions within their session. This can lead to unauthorized data modification such as credential updates.	6.8	More Details
CVE-2025-65731	An issue was discovered in D-Link Router DIR-605L (Hardware version F1; Firmware version: V6.02CN02) allowing an attacker with physical access to the UART pins to execute arbitrary commands due to presence of root terminal access on a serial interface without proper access control.	6.8	More Details
CVE-2025-66837	A file upload vulnerability in ARIS 10.0.23.0.3587512 allows attackers to execute arbitrary code via uploading a crafted PDF file/Malware	6.8	More Details
CVE-2026-22801	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From 1.6.26 to 1.6.53, there is an integer truncation in the libpng simplified write API functions png_write_image_16bit and png_write_image_8bit causes heap buffer over-read when the caller provides a negative row stride (for bottom-up image layouts) or a stride exceeding 65535 bytes. The bug was introduced in libpng 1.6.26 (October 2016) by casts added to silence compiler warnings on 16-bit systems. This vulnerability is fixed in 1.6.54.	6.8	More Details
CVE-2025-14803	The NEX-Forms WordPress plugin before 9.1.8 does not sanitise and escape some of its settings. The NEX-Forms WordPress plugin before 9.1.8 can be configured in such a way that could allow subscribers to perform Stored Cross-Site Scripting.	6.8	More Details
CVE-2026-21694	Titra is open source project time tracking software. Versions 0.99.49 and below have Improper Access Control, allowing users to view and edit other users' time entries in private projects they have not been granted access to. This issue is fixed in version 0.99.50.	6.8	More Details
CVE-2025-68622	Espressif ESP-IDF USB Host UVC Class Driver allows video streaming from USB cameras. Prior to 2.4.0, a vulnerability in the esp-usb UVC host implementation allows a malicious USB Video Class (UVC) device to trigger a stack buffer overflow during configuration-descriptor parsing. When UVC configuration-descriptor printing is enabled, the host prints detailed descriptor information provided by the connected USB device. A specially crafted UVC descriptor may advertise an excessively large length. Because this value is not validated before being copied into a fixed-size stack buffer, an attacker can overflow the buffer and corrupt memory. This vulnerability is fixed in 2.4.0.	6.8	More Details
CVE-2025-68656	Espressif ESP-IDF USB Host HID (Human Interface Device) Driver allows access to HID devices. Prior to 1.1.0, usb_class_request_get_descriptor() frees and reallocates hid_device->ctrl_xfer when an oversized descriptor is requested but continues to use the stale local pointer, leading to an immediate use-after-free when processing attacker-controlled Report Descriptor lengths. This vulnerability is fixed in 1.1.0.	6.8	More Details
CVE-2025-14599	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Standard Installer (SFX) on Windows, Altera Quartus Prime Lite Installer (SFX) on Windows allows Search Order Hijacking.This issue affects Quartus Prime Standard: from 23.1 through 24.1; Quartus Prime Lite: from 23.1 through 24.1.	6.7	More Details
CVE-2026-22596	Ghost is a Node.js content management system. In versions 5.90.0 through 5.130.5 and 6.0.0 through 6.10.3, a vulnerability in Ghost's /ghost/api/admin/members/events endpoint allows users with authentication credentials for the Admin API to execute arbitrary SQL. This issue has been patched in versions 5.130.6 and 6.11.0.	6.7	More Details
CVE-2026-20876	Heap-based buffer overflow in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-14596	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Pro Installer (SFX) on Windows allows Search Order Hijacking.This issue affects Quartus Prime Pro: from 24.1 through 24.3.1.	6.7	More Details

CVE-2025-47337	Memory corruption while accessing a synchronization object during concurrent operations.	6.7	More Details
CVE-2025-14605	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Pro on Windows (System Console modules) allows Search Order Hijacking.This issue affects Quartus Prime Pro: from 17.0 through 25.1.1.	6.7	More Details
CVE-2025-47335	Memory corruption while parsing clock configuration data for a specific hardware type.	6.7	More Details
CVE-2025-47336	Memory corruption while performing sensor register read operations.	6.7	More Details
CVE-2025-47334	Memory corruption while processing shared command buffer packet between camera userspace and kernel.	6.7	More Details
CVE-2025-47344	Memory corruption while handling sensor utility operations.	6.7	More Details
CVE-2025-47332	Memory corruption while processing a config call from userspace.	6.7	More Details
CVE-2025-14612	Insecure Temporary File vulnerability in Altera Quartus Prime Pro Installer (SFX) on Windows allows : Use of Predictable File Names.This issue affects Quartus Prime Pro: from 24.1 through 25.1.1.	6.7	More Details
CVE-2025-14614	Insecure Temporary File vulnerability in Altera Quartus Prime Standard Installer (SFX) on Windows, Altera Quartus Prime Lite Installer (SFX) on Windows allows Explore for Predictable Temporary File Names.This issue affects Quartus Prime Standard: from 23.1 through 24.1; Quartus Prime Lite: from 23.1 through 24.1.	6.7	More Details
CVE-2025-14625	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Standard on Windows (Nios II Command Shell modules), Altera Quartus Prime Lite on Windows (Nios II Command Shell modules) allows Search Order Hijacking.This issue affects Quartus Prime Standard: from 19.1 through 24.1; Quartus Prime Lite: from 19.1 through 24.1.	6.7	More Details
CVE-2026-22791	openCryptoki is a PKCS#11 library and tools for Linux and AIX. In 3.25.0 and 3.26.0, there is a heap buffer overflow vulnerability in the CKM_ECDH_AES_KEY_WRAP implementation allows an attacker with local access to cause out-of-bounds writes in the host process by supplying a compressed EC public key and invoking C_WrapKey. This can lead to heap corruption, or denial-of-service.	6.6	More Details
CVE-2026-21504	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to heap buffer overflow in the ToneMap parser. This issue has been patched in version 2.3.1.2.	6.6	More Details
CVE-2025-47333	Memory corruption while handling buffer mapping operations in the cryptographic driver.	6.6	More Details
CVE-2025-46684	Dell SupportAssist OS Recovery, versions prior to 5.5.15.1, contain a Creation of Temporary File With Insecure Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information Tampering.	6.6	More Details
CVE-2026-0496	SAP Fiori App Intercompany Balance Reconciliation allows an attacker with high privileges to upload any file (including script files) without proper file format validation. This has low impact on confidentiality, integrity and availability of the application.	6.6	More Details
CVE-2025-37177	An arbitrary file deletion vulnerability has been identified in the command-line interface of mobility conductors running either AOS-10 or AOS-8 operating systems. Successful exploitation of this vulnerability could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	6.5	More Details
CVE-2025-67004	An Information Disclosure vulnerability in CouchCMS 2.4 allow an Admin user to read arbitrary files via traversing directories back after back. It can Disclosure the source code or any other confidential information if weaponize accordingly.	6.5	More Details
CVE-2025-	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_order_by_id() function in all versions up to, and including, 3.9.3. This makes it possible for authenticated attackers, with Subscriber-level access and above,	6.5	More

13679	to enumerate order IDs and exfiltrate sensitive data (PII), such as student name, email address, phone number, and billing address.		Details
CVE-2025-37176	A command injection vulnerability in AOS-8 allows an authenticated privileged user to alter a package header to inject shell commands, potentially affecting the execution of internal operations. Successful exploit could allow an authenticated malicious actor to execute commands with the privileges of the impacted mechanism.	6.5	More Details
CVE-2025-66689	A path traversal vulnerability exists in Zen MCP Server before 9.8.2 that allows authenticated attackers to read arbitrary files on the system. The vulnerability is caused by flawed logic in the is_dangerous_path() validation function that uses exact string matching against a blacklist of system directories. Attackers can bypass these restrictions by accessing subdirectories of blacklisted paths.	6.5	More Details
CVE-2025-66715	A DLL hijacking vulnerability in Axtion ODISSAAS ODIS v1.8.4 allows attackers to execute arbitrary code via a crafted DLL file.	6.5	More Details
CVE-2025-14901	The Bit Form – Contact Form Plugin plugin for WordPress is vulnerable to unauthorized workflow execution due to missing authorization in the triggerWorkFlow function in all versions up to, and including, 2.21.6. This is due to a logic flaw in the nonce verification where the security check only blocks requests when both the nonce verification fails and the user is logged in. This makes it possible for unauthenticated attackers to replay form workflow executions and trigger all configured integrations including webhooks, email notifications, CRM integrations, and automation platforms via the bitforms_trigger_workflow AJAX action granted they can obtain the entry ID and log IDs from a legitimate form submission response.	6.5	More Details
CVE-2025-67811	Area9 Rhapsode 1.47.3 allows SQL Injection via multiple API endpoints accessible to authenticated users. Insufficient input validation allows remote attackers to inject arbitrary SQL commands, resulting in unauthorized database access and potential compromise of sensitive data. Fixed in v.1.47.4 and beyond.	6.5	More Details
CVE-2025-46645	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS 2023 release versions 7.10.1.0 through 7.10.1.70, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	6.5	More Details
CVE-2025-68468	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. In 0.9-rc2 and earlier, avahi-daemon can be crashed by sending unsolicited announcements containing CNAME resource records pointing it to resource records with short TTLs. As soon as they expire avahi-daemon crashes.	6.5	More Details
CVE-2025-68471	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. In 0.9-rc2 and earlier, avahi-daemon can be crashed by sending 2 unsolicited announcements with CNAME resource records 2 seconds apart.	6.5	More Details
CVE-2025-67278	An issue in TIM Solution GmbH TIM BPM Suite & TIM FLOW before v.9.1.2 allows a remote attacker to escalate privileges via a crafted HTTP request	6.5	More Details
CVE-2026-0528	Improper Validation of Array Index (CWE-129) exists in Metricbeat can allow an attacker to cause a Denial of Service through Input Data Manipulation (CAPEC-153) via specially crafted, malformed payloads sent to the Graphite server metricset or Zookeeper server metricset. Additionally, Improper Input Validation (CWE-20) exists in the Prometheus helper module that can allow an attacker to cause a Denial of Service through Input Data Manipulation (CAPEC-153) via specially crafted, malformed metric data.	6.5	More Details
CVE-2026-0530	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana Fleet can lead to Excessive Allocation (CAPEC-130) via a specially crafted request. This causes the application to perform redundant processing operations that continuously consume system resources until service degradation or complete unavailability occurs.	6.5	More Details
CVE-2026-0543	Improper Input Validation (CWE-20) in Kibana's Email Connector can allow an attacker to cause an Excessive Allocation (CAPEC-130) through a specially crafted email address parameter. This requires an attacker to have authenticated access with view-level privileges sufficient to execute connector actions. The application attempts to process specially crafted email format, resulting in complete service unavailability for all users until manual restart is performed.	6.5	More Details
CVE-2025-14172	The WP Page Permalink Extension plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.5.4. This is due to missing authorization checks on the `cwpp_trigger_flush_rewrite_rules` function hooked to `wp_ajax_cwpp_trigger_flush_rewrite_rules`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to flush the site's rewrite rules via the `action` parameter.	6.5	More Details
CVE-2025-	GitLab has remediated an issue in GitLab EE affecting all versions from 18.5 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed an authenticated user to modify instance-wide AI	6.5	More Details

13781	feature provider settings by exploiting missing authorization checks in GraphQL mutations.		
CVE-2025-10569	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.3 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed an authenticated user to create a denial of service condition by providing crafted responses to external API calls.	6.5	More Details
CVE-2026-21680	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a NULL pointer dereference vulnerability. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	6.5	More Details
CVE-2025-67810	In Area9 Rhapsode 1.47.3, an authenticated attacker can exploit the operation, url, and filename parameters via POST request to read arbitrary files from the server filesystem. Fixed in 1.47.4 (#7254) and further versions.	6.5	More Details
CVE-2025-65553	D3D Wi-Fi Home Security System ZX-G12 v2.1.17 is susceptible to RF jamming on the 433 MHz alarm sensor channel. An attacker within RF range can transmit continuous interference to block sensor transmissions, resulting in missed alarms and loss of security monitoring. The device lacks jamming detection or mitigations, creating a denial-of-service condition that may lead to undetected intrusions or failure to trigger safety alerts.	6.5	More Details
CVE-2025-51626	SQL injection vulnerability in pss.sale.com 1.0 via the id parameter to the userfiles/php/cancel_order.php endpoint.	6.5	More Details
CVE-2025-60538	A lack of rate limiting in the login page of shiori v1.7.4 and below allows attackers to bypass authentication via a brute force attack.	6.5	More Details
CVE-2026-20872	External control of file name or path in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-46434	Missing Authorization vulnerability in POSIMYTH Innovation The Plus Addons for Elementor Pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Plus Addons for Elementor Pro: from n/a before 6.3.7.	6.5	More Details
CVE-2026-20925	External control of file name or path in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-66838	In Aris v10.0.23.0.3587512 and before, the file upload functionality does not enforce any rate limiting or throttling, allowing users to upload files at an unrestricted rate. An attacker can exploit this behavior to rapidly upload a large volume of files, potentially leading to resource exhaustion such as disk space depletion, increased server load, or degraded performance	6.5	More Details
CVE-2025-4675	Improper Check for Unusual or Exceptional Conditions vulnerability in ABB WebPro SNMP Card PowerValue, ABB WebPro SNMP Card PowerValue UL.This issue affects WebPro SNMP Card PowerValue: through 1.1.8.K; WebPro SNMP Card PowerValue UL: through 1.1.8.K.	6.5	More Details
CVE-2026-22773	vLLM is an inference and serving engine for large language models (LLMs). In versions from 0.6.4 to before 0.12.0, users can crash the vLLM engine serving multimodal models that use the Idefics3 vision model implementation by sending a specially crafted 1x1 pixel image. This causes a tensor dimension mismatch that results in an unhandled runtime error, leading to complete server termination. This issue has been patched in version 0.12.0.	6.5	More Details
CVE-2025-61489	A command injection vulnerability in the shell_exec function of sonirico mcp-shell v0.3.1 allows attackers to execute arbitrary commands via supplying a crafted command string.	6.5	More Details
CVE-2025-68867	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in anibalwainstein Effect Maker effect-maker allows DOM-Based XSS.This issue affects Effect Maker: from n/a through <= 1.2.1.	6.5	More Details
CVE-2025-4677	Insufficient Session Expiration vulnerability in ABB WebPro SNMP Card PowerValue, ABB WebPro SNMP Card PowerValue UL.This issue affects WebPro SNMP Card PowerValue: through 1.1.8.K; WebPro SNMP Card PowerValue UL: through 1.1.8.K.	6.5	More Details
CVE-2026-22689	Mailpit is an email testing tool and API for developers. Prior to version 1.28.2, the Mailpit WebSocket server is configured to accept connections from any origin. This lack of Origin header validation introduces a Cross-Site WebSocket Hijacking (CSWSH) vulnerability. An attacker can host a malicious website that, when visited by a developer running Mailpit locally, establishes a WebSocket connection to the victim's Mailpit instance (default ws://localhost:8025). This allows the attacker to intercept sensitive data such as email contents, headers, and server statistics in real-time. This issue has been patched in version 1.28.2.	6.5	More Details

CVE-2025-47395	Transient DOS while parsing a WLAN management frame with a Vendor Specific Information Element.	6.5	More Details
CVE-2026-20847	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-22030	React Router is a router for React. In @remix-run/server-runtime version prior to 2.17.3. and react-router 7.0.0 through 7.11.0, React Router (or Remix v2) is vulnerable to CSRF attacks on document POST requests to UI routes when using server-side route action handlers in Framework Mode, or when using React Server Actions in the new unstable RSC modes. There is no impact if Declarative Mode (<BrowserRouter>) or Data Mode (createBrowserRouter/<RouterProvider>) is being used. This issue has been patched in @remix-run/server-runtime version 2.17.3 and react-router version 7.12.0.	6.5	More Details
CVE-2025-68470	React Router is a router for React. In versions 6.0.0 through 6.30.1 and 7.0.0 through 7.9.5, an attacker-supplied path can be crafted so that when a React Router application navigates to it via navigate(), <Link>, or redirect(), the app performs a navigation/redirect to an external URL. This is only an issue if you are passing untrusted content into navigation paths in your application code. This issue has been patched in versions 6.30.2 and 7.9.6.	6.5	More Details
CVE-2026-21894	n8n is an open source workflow automation platform. In versions from 0.150.0 to before 2.2.2, an authentication bypass vulnerability in the Stripe Trigger node allows unauthenticated parties to trigger workflows by sending forged Stripe webhook events. The Stripe Trigger creates and stores a Stripe webhook signing secret when registering the webhook endpoint, but incoming webhook requests were not verified against this secret. As a result, any HTTP client that knows the webhook URL could send a POST request containing a matching event type, causing the workflow to execute as if a legitimate Stripe event had been received. This issue affects n8n users who have active workflows using the Stripe Trigger node. An attacker could potentially fake payment or subscription events and influence downstream workflow behavior. The practical risk is reduced by the fact that the webhook URL contains a high-entropy UUID; however, authenticated n8n users with access to the workflow can view this webhook ID. This issue has been patched in version 2.2.2. A temporary workaround for this issue involves users deactivating affected workflows or restricting access to workflows containing Stripe Trigger nodes to trusted users only.	6.5	More Details
CVE-2025-14867	The Flashcard plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 0.9 via the 'source' attribute of the 'flashcard' shortcode. This makes it possible for authenticated attackers, with contributor level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-14059	The EmailKit plugin for WordPress is vulnerable to Arbitrary File Read via Path Traversal in all versions up to, and including, 1.6.1. This is due to missing path validation in the create_template REST API endpoint where user-controlled input from the emailkit-editor-template parameter is passed directly to file_get_contents() without sanitization. This makes it possible for authenticated attackers with Author-level permissions or higher to read arbitrary files on the server, including sensitive configuration files like /etc/passwd and wp-config.php, via the REST API. The file contents are stored in post meta and can be exfiltrated through MetForm's email confirmation feature.	6.5	More Details
CVE-2025-46298	The issue was addressed with improved memory handling. This issue is fixed in tvOS 26.2, Safari 26.2, watchOS 26.2, visionOS 26.2, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2. Processing maliciously crafted web content may lead to an unexpected process crash.	6.5	More Details
CVE-2026-21885	Miniflux 2 is an open source feed reader. Prior to version 2.2.16, Miniflux's media proxy endpoint (`GET /proxy/{encodedDigest}/{encodedURL}`) can be abused to perform Server-Side Request Forgery (SSRF). An authenticated user can cause Miniflux to generate a signed proxy URL for attacker-chosen media URLs embedded in feed entry content, including internal addresses (e.g., localhost, private RFC1918 ranges, or link-local metadata endpoints). Requesting the resulting `/proxy/...` URL makes Miniflux fetch and return the internal response. Version 2.2.16 fixes the issue.	6.5	More Details
CVE-2022-50899	Geonetwork 3.10 through 4.2.0 contains an XML external entity vulnerability in PDF rendering that allows attackers to retrieve arbitrary files from the server. Attackers can exploit the insecure XML parser by crafting a malicious XML document with external entity references to read system files through the baseURL parameter in PDF creation requests.	6.5	More Details
CVE-2026-0531	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana Fleet can lead to Excessive Allocation (CAPEC-130) via a specially crafted bulk retrieval request. This requires an attacker to have low-level privileges equivalent to the viewer role, which grants read access to agent policies. The crafted request can cause the application to perform redundant database retrieval operations that immediately consume memory until the server crashes and becomes unavailable to all users.	6.5	More Details
CVE-2019-25295	The WP Cost Estimation plugin for WordPress is vulnerable to Upload Directory Traversal in versions before 9.660 via the uploadFormFiles function. This allows attackers to overwrite any file with a whitelisted type on an affected site.	6.5	More Details

CVE-2025-14980	The BetterDocs plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.3 via the scripts() function. This makes it possible for authenticated attackers, with contributor-level access and above, to extract sensitive data including the OpenAI API key stored in plugin settings.	6.5	More Details
CVE-2025-58693	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiVoice 7.2.0 through 7.2.2, FortiVoice 7.0.0 through 7.0.7 allows a privileged attacker to delete files from the underlying filesystem via crafted HTTP or HTTPs requests.	6.5	More Details
CVE-2026-21689	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `CIccProfileXml::ParseBasic()` at `IccXML/IccLibXML/IccProfileXml.cpp`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	6.5	More Details
CVE-2026-20812	Improper input validation in Windows LDAP - Lightweight Directory Access Protocol allows an authorized attacker to perform tampering over a network.	6.5	More Details
CVE-2026-22519	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev MediaPress allows Stored XSS.This issue affects MediaPress: from n/a through 1.6.2.	6.5	More Details
CVE-2026-0890	Spoofing issue in the DOM: Copy & Paste and Drag & Drop component. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	6.5	More Details
CVE-2026-22588	Spree is an open source e-commerce solution built with Ruby on Rails. Prior to versions 4.10.2, 5.0.7, 5.1.9, and 5.2.5, an Authenticated Insecure Direct Object Reference (IDOR) vulnerability was identified that allows an authenticated user to retrieve other users' address information by modifying an existing order. By editing an order they legitimately own and manipulating address identifiers in the request, the backend server accepts and processes references to addresses belonging to other users, subsequently associating those addresses with the attacker's order and returning them in the response. This issue has been patched in versions 4.10.2, 5.0.7, 5.1.9, and 5.2.5.	6.5	More Details
CVE-2025-64305	MicroServer copies parts of the system firmware to an unencrypted external SD card on boot, which contains user and vendor secrets. An attacker can utilize these plaintext secrets to modify the vendor firmware, or gain admin access to the web portal.	6.5	More Details
CVE-2026-22522	Missing Authorization vulnerability in Munir Kamal Block Slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Block Slider: from n/a through 2.2.3.	6.5	More Details
CVE-2026-22246	Mastodon is a free, open-source social network server based on ActivityPub. Mastodon 4.3 added notifications of severed relationships, allowing end-users to inspect the relationships they lost as the result of a moderation action. The code allowing users to download lists of severed relationships for a particular event fails to check the owner of the list before returning the lost relationships. Any registered local user can access the list of lost followers and followed users caused by any severance event, and go through all severance events this way. The leaked information does not include the name of the account which has lost follows and followers. This has been fixed in Mastodon v4.3.17, v4.4.11 and v4.5.4.	6.5	More Details
CVE-2026-22518	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pencilwp X Addons for Elementor allows DOM-Based XSS.This issue affects X Addons for Elementor: from n/a through 1.0.23.	6.5	More Details
CVE-2025-67091	An issue in GL Inet GL.Inet AX1800 Version 4.6.4 & 4.6.8 are vulnerable. GL.Inet AX1800 Version 4.6.4 & 4.6.8 in the GL.iNet custom opkg wrapper script located at /usr/libexec/opkg-call. The script is executed with root privileges when triggered via the LuCI web interface or authenticated API calls to manage packages. The vulnerable code uses shell redirection to create a lock file in the world-writable /tmp directory.	6.5	More Details
CVE-2026-0885	Use-after-free in the JavaScript: GC component. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	6.5	More Details
CVE-2025-14110	The WP Js List Pages Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' shortcode attribute in all versions up to, and including, 1.21 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-2025-14112	The Snillrik Restaurant plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'menu_style' shortcode attribute in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-13418	The Responsive Pricing Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'plan_icons' parameter in all versions up to, and including, 5.1.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13897	The Client Testimonial Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'aft_testimonial_meta_name' custom field in the Client Information metabox in all versions up to, and including, 2.0 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 the injected administrative page.	6.4	More Details
CVE-2025-13903	The PullQuote plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'pullquote' shortcode in all versions up to, and including, 1.0 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-2025-13908	The The Tooltip plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'the_tooltip' shortcode in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13967	The Woodpecker for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_name' parameter of the [woodpecker-connector] shortcode in all versions up to, and including, 3.0.4 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-2022-50906	e107 CMS 3.2.1 contains an upload restriction bypass vulnerability that allows authenticated administrators to upload malicious SVG files through the media manager. Attackers with admin privileges can exploit this vulnerability to upload SVG files with embedded cross-site scripting (XSS) payloads that can execute arbitrary scripts when viewed.	6.4	More Details
CVE-2026-0563	The WP Google Street View (with 360° virtual tour) & Google maps + Local SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpgsv_map' shortcode in all versions up to, and including, 1.1.8 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-2025-13497	The Recras WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'recrasname' shortcode attribute in all versions up to, and including, 6.4.1. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13887	The AI BotKit – AI Chatbot & Live Support for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in the `ai_botkit_widget` shortcode in all versions up to, and including, 1.1.7 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-2025-13531	The Stylish Order Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'product_name' parameter in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-46256	Path Traversal: '.../...//' vulnerability in SigmaPlugin Advanced Database Cleaner PRO allows Path Traversal.This issue affects Advanced Database Cleaner PRO: from n/a through 3.2.10.	6.4	More Details
CVE-2025-14984	The Gutenverse Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file upload in all versions up to, and including, 2.3.2. This is due to the plugin's framework component adding SVG to the allowed MIME types via the upload_mimes filter without implementing any sanitization of SVG file contents. This makes it possible for authenticated attackers, with Author-level access and above, to upload SVG files containing malicious JavaScript that executes when the file is viewed, leading to arbitrary JavaScript execution in victims' browsers.	6.4	More Details
CVE-2025-14506	The ConvertForce Popup Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Gutenberg block's `entrance_animation` attribute in all versions up to, and including, 0.0.7. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
	The My Album Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'style_css'		

CVE-2025-14453	shortcode attribute in all versions up to, and including, 1.0.4 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-2025-13667	The WP Recipe Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Skill Level' input field in all versions up to, and including, 1.0.0 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-2025-13848	The STM Gallery 1.9 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'composicion' parameter in all versions up to, and including, 0.9 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-2025-14144	The Mstoic Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'start' parameter of the ms_youtube_embeds shortcode in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14145	The Niche Hero | Beautifully-designed blocks in seconds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'spacing' parameter of the nh_row shortcode in all versions up to, and including, 1.0.5 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-2025-13847	The PhotoFade plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'time' parameter in all versions up to, and including, 0.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12379	The Shortcodes and extra features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a combination of the 'tag' and ‘title_tag’ parameters in all versions up to, and including, 2.17.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13849	The Cool YT Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'videoid' parameter in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-68657	Espressif ESP-IDF USB Host HID (Human Interface Device) Driver allows access to HID devices. Prior to 1.1.0, calls to hid_host_device_close() can free the same usb_transfer_t twice. The USB event callback and user code share the hid_iface_t state without locking, so both can tear down a READY interface simultaneously, corrupting heap metadata inside the ESP USB host stack. This vulnerability is fixed in 1.1.0.	6.4	More Details
CVE-2025-14555	The Countdown Timer – Widget Countdown plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdevart_countdown' shortcode in all versions up to, and including, 2.7.7 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-2025-13841	The Smart App Banners plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'size' and 'verticalalign' parameters of the 'app-store-download' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14147	The Easy GitHub Gist Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the gist shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13862	The Menu Card plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `category` parameter in all versions up to, and including, 0.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-	The Curved Text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'radius' parameter of the arctext shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and		More

2025-13854	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	Details
CVE-2025-13852	The Debt.com Business in a Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'configuration' parameter of the lead_form shortcode in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-15019	The BIALTY - Bulk Image Alt Text (Alt tag, Alt Attribute) with Yoast SEO + WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bialty_cs_alt' post meta in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the post editor.	6.4	More Details
CVE-2026-22705	RustCrypto: Signatures offers support for digital signatures, which provide authentication of data using public-key cryptography. Prior to version 0.1.0-rc.2, a timing side-channel was discovered in the Decompose algorithm which is used during ML-DSA signing to generate hints for the signature. This issue has been patched in version 0.1.0-rc.2.	6.4	More Details
CVE-2025-14275	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.0.1 due to insufficient input sanitization in the countdown widget's redirect functionality. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary JavaScript that will execute when an administrator or other user views the page containing the malicious countdown element.	6.4	More Details
CVE-2025-14113	The Viitor Button Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' shortcode attribute in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14114	The 1180px Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' shortcode attribute in all versions up to, and including, 1.1.1 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-2026-0503	Due to missing authorization check in the SAP ERP Central Component (SAP ECC) and SAP S/4HANA (SAP EHS Management), an attacker could extract hardcoded clear-text credentials and bypass the password authentication check by manipulating user parameters. Upon successful exploitation, the attacker can access, modify or delete certain change pointer information within EHS objects in the application which might further affect the subsequent systems. This vulnerability leads to a low impact on confidentiality and integrity of the application with no affect on the availability.	6.4	More Details
CVE-2025-0980	Nokia SR Linux is vulnerable to an authentication vulnerability allowing unauthorized access to the JSON-RPC service. When exploited, an invalid validation allows JSON RPC access without providing valid authentication credentials.	6.4	More Details
CVE-2025-14121	The EDD Download Info plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'edd_download_info_link' shortcode in all versions up to, and including, 1.1 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-2026-0627	The AMP for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file uploads in all versions up to, and including, 1.1.10. This is due to insufficient sanitization of SVG file content that only removes `<script>` tags while allowing other XSS vectors such as event handlers (onload, onerror, onmouseover), foreignObject elements, and SVG animation attributes. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts via malicious SVG file uploads that will execute whenever a user views the uploaded file.	6.4	More Details
CVE-2025-14893	The IndieWeb plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Telephone' parameter in all versions up to, and including, 4.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14109	The AH Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'column' shortcode attribute in all versions up to, and including, 1.0.2 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
	The Entry Views plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'entry-views'		

CVE-2025-13729	shortcode in all versions up to, and including, 1.0.0 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-2025-14122	The AD Sliding FAQ plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sliding_faq' shortcode in all versions up to, and including, 2.4 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-2025-15058	The Responsive Pricing Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'table_currency' parameter in all versions up to, and including, 5.1.12 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-2025-13853	The Nearby Now Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data_tech' parameter of the nn-tech shortcode in all versions up to, and including, 5.2 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-2026-21265	Windows Secure Boot stores Microsoft certificates in the UEFI KEK and DB. These original certificates are approaching expiration, and devices containing affected certificate versions must update them to maintain Secure Boot functionality and avoid compromising security by losing security fixes related to Windows boot manager or Secure Boot. The operating system’s certificate update protection mechanism relies on firmware components that might contain defects, which can cause certificate trust updates to fail or behave unpredictably. This leads to potential disruption of the Secure Boot trust chain and requires careful validation and deployment to restore intended security guarantees. Certificate Authority (CA) Location Purpose Expiration Date Microsoft Corporation KEK CA 2011 KEK Signs updates to the DB and DBX 06/24/2026 Microsoft Corporation UEFI CA 2011 DB Signs 3rd party boot loaders, Option ROMs, etc. 06/27/2026 Microsoft Windows Production PCA 2011 DB Signs the Windows Boot Manager 10/19/2026 For more information see this CVE and Windows Secure Boot certificate expiration and CA updates.	6.4	More Details
CVE-2025-13900	The WP Popup Magic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter of the [wppum_end] shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14891	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'displayName' parameter in all versions up to, and including, 5.93.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with customer-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. While it is possible to invoke the AJAX action without authentication, the attacker would need to know a valid form ID, which requires them to place an order. This vulnerability can be exploited by unauthenticated attackers if guest checkout is enabled. However, the form ID still needs to be obtained through placing an order.	6.4	More Details
CVE-2025-14796	The My Album Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image titles in all versions up to, and including, 1.0.4. This is due to insufficient input sanitization and output escaping on the 'attachment->title' attribute. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14053	The Wish To Go plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcode attributes in all versions up to, and including, 0.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11453	The Header and Footer Scripts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _inpost_head_script parameter in all versions up to, and including, 2.2.2 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-2024-54855	fabricators Ltd Vanilla OS 2 Core image v1.1.0 was discovered to contain static keys for the SSH service, allowing attackers to possibly execute a man-in-the-middle attack during connections with other hosts.	6.4	More Details
CVE-2025-13704	The Autogen Headers Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'head_class' parameter of the 'autogen_menu' shortcode in all versions up to, and including, 1.0.1 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-2025-14626	The QR Code for WooCommerce order emails, PDF invoices, packing slips plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode in all versions up to, and including, 1.9.42 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-2026-0733	A vulnerability was determined in PHPGurukul Online Course Registration System up to 3.1. This impacts an unknown function of the file /onlinecourse/admin/manage-students.php. This manipulation of the argument id/cid causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-21690	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `CIccTagXmlTagData::ToXml()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	6.3	More Details
CVE-2025-15494	A vulnerability has been found in RainyGao DocSys up to 2.02.37. This affects an unknown function of the file com/DocSystem/mapping/UserMapper.xml. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-15496	A vulnerability was determined in guchengwuyue yshopmall up to 1.9.1. Affected is the function getPage of the file /api/jobs. This manipulation of the argument sort causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-0732	A vulnerability was found in D-Link DI-8200G 17.12.20A1. This affects an unknown function of the file /upgrade_filter.asp. The manipulation of the argument path results in command injection. The attack may be performed from remote. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-0842	A flaw has been found in Flycatcher Toys smART Sketcher up to 2.0. This affects an unknown part of the component Bluetooth Low Energy Interface. This manipulation causes missing authentication. The attack can only be done within the local network. 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-2025-15493	A flaw has been found in RainyGao DocSys up to 2.02.36. The impacted element is an unknown function of the file src/com/DocSystem/mapping/ReposAuthMapper.xml. Executing a manipulation of the argument searchWord can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-0822	A vulnerability was identified in quickjs-ng quickjs up to 0.11.0. This issue affects the function js_typed_array_sort of the file quickjs.c. The manipulation leads to heap-based buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The identifier of the patch is 53eefbcd695165a3bd8c584813b472cb4a69fbf5. To fix this issue, it is recommended to deploy a patch.	6.3	More Details
CVE-2026-0803	A vulnerability was found in PHPGurukul Online Course Registration System up to 3.1. This affects an unknown part of the file /enroll.php. The manipulation of the argument studentregno/Pincode/session/department/level/course/sem results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-15492	A vulnerability was detected in RainyGao DocSys up to 2.02.36. The affected element is an unknown function of the file src/com/DocSystem/mapping/GroupMemberMapper.xml. Performing a manipulation of the argument searchWord results in sql injection. It is possible to initiate the attack 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-2026-0843	A vulnerability has been found in jiujiujia/victor123/wxw850227 jjjfood and jjjshop_food up to 20260103. This vulnerability affects unknown code of the file /index.php/api/product.category/index. Such manipulation of the argument latitude leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product is distributed under multiple different names. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-20851	Out-of-bounds read in Capability Access Management Service (camsvc) allows an unauthorized attacker to disclose information locally.	6.2	More Details
CVE-2022-50897	mPDF 7.0 contains a local file inclusion vulnerability that allows attackers to read arbitrary system files by manipulating annotation file parameters. Attackers can generate URL-encoded or base64 payloads to include local files through crafted annotation content with file path specifications.	6.2	More Details

CVE-2022-50891	Owlfiles File Manager 12.0.1 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through the path parameter in HTTP server endpoints. Attackers can craft URLs targeting the download and list endpoints with embedded script tags to execute arbitrary JavaScript in users' browsers.	6.2	More Details
CVE-2026-20818	Insertion of sensitive information into log file in Windows Kernel allows an unauthorized attacker to disclose information locally.	6.2	More Details
CVE-2026-20935	Untrusted pointer dereference in Windows Virtualization-Based Security (VBS) Enclave allows an unauthorized attacker to disclose information locally.	6.2	More Details
CVE-2021-47749	YouPHPTube <= 7.8 contains a local file inclusion vulnerability that allows unauthenticated attackers to access arbitrary files by manipulating the 'lang' parameter in GET requests. Attackers can exploit the path traversal flaw in locale/function.php to include and view PHP files outside the intended directory by using directory traversal sequences.	6.2	More Details
CVE-2026-20821	Exposure of sensitive information to an unauthorized actor in Windows Remote Procedure Call allows an unauthorized attacker to disclose information locally.	6.2	More Details
CVE-2017-20212	FLIR Thermal Camera F/FC/PT/D firmware version 8.0.0.64 contains an information disclosure vulnerability that allows unauthenticated attackers to read arbitrary files through unverified input parameters. Attackers can exploit the /var/www/data/controllers/api/xml.php readFile() function to access local system files without authentication.	6.2	More Details
CVE-2025-8090	Null pointer dereference in the MsgRegisterEvent() system call could allow an attacker with local access and code execution abilities to crash the QNX Neutrino kernel.	6.2	More Details
CVE-2022-50927	Cyclades Serial Console Server 3.3.0 contains a local privilege escalation vulnerability due to overly permissive sudo privileges for the admin user and admin group. Attackers can exploit the default user configuration to gain root access by manipulating system binaries and leveraging unrestricted sudo permissions.	6.2	More Details
CVE-2025-61674	October is a Content Management System (CMS) and web platform. Prior to versions 3.7.13 and 4.0.12, a cross-site scripting (XSS) vulnerability was identified in October CMS backend configuration forms. A user with the Global Editor Settings permission could inject malicious HTML/JS into the stylesheet input at Markup Styles. A specially crafted input could break out of the intended <style> context, allowing arbitrary script execution across backend pages for all users. This issue has been patched in versions 3.7.13 and 4.0.12.	6.1	More Details
CVE-2025-14118	The Starred Review plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the PHP_SELF variable in all versions up to, and including, 1.4.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-67933	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in taskbuilder Taskbuilder taskbuilder allows Reflected XSS.This issue affects Taskbuilder: from n/a through <= 4.0.9.	6.1	More Details
CVE-2022-50896	Testa 3.5.1 contains a reflected cross-site scripting vulnerability in the login.php redirect parameter that allows attackers to inject malicious scripts. Attackers can craft a specially encoded payload in the redirect parameter to execute arbitrary JavaScript in victim's browser context.	6.1	More Details
CVE-2026-21872	NiceGUI is a Python-based UI framework. From versions 2.22.0 to 3.4.1, an unsafe implementation in the click event listener used by ui.sub_pages, combined with attacker-controlled link rendering on the page, causes XSS when the user actively clicks on the link. This issue has been patched in version 3.5.0.	6.1	More Details
CVE-2026-21871	NiceGUI is a Python-based UI framework. From versions 2.13.0 to 3.4.1, there is a XSS risk in NiceGUI when developers pass attacker-controlled strings into ui.navigate.history.push() or ui.navigate.history.replace(). These helpers are documented as History API wrappers for updating the browser URL without page reload. However, if the URL argument is embedded into generated JavaScript without proper escaping, a crafted payload can break out of the intended string context and execute arbitrary JavaScript in the victim’s browser. Applications that do not pass untrusted input into ui.navigate.history.push/replace are not affected. This issue has been patched in version 3.5.0.	6.1	More Details
CVE-2025-61549	Cross-Site Scripting (XSS) is present on the LoginID parameter on the /PSP/app/web/reg/reg_display.asp endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34. Unsanitized user input is reflected in HTTP responses without proper HTML encoding or escaping. This allows attackers to execute arbitrary JavaScript in the context of a victim s browser session	6.1	More Details
CVE-	A stored Cross-Site Scripting (XSS) vulnerability exists in Perch CMS version 3.2. An authenticated attacker with administrative privileges can inject malicious JavaScript code into the “Help button url” setting within the		More

2025-66686	admin panel. The injected payload is stored and executed when any authenticated user clicks the Help button, potentially leading to session hijacking, information disclosure, privilege escalation, and unauthorized administrative actions.	6.1	Details
CVE-2026-0499	SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to inject malicious scripts into a URL parameter. The scripts are reflected in the server response and executed in a user's browser when the crafted URL is visited, leading to theft of session information, manipulation of portal content, or user redirection, resulting in a low impact on the application's confidentiality and integrity, with no impact on availability.	6.1	More Details
CVE-2026-21503	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV has undefined behavior due to a null pointer passed to memcpy() in CIccTagSparseMatrixArray. This issue has been patched in version 2.3.1.2.	6.1	More Details
CVE-2026-0671	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki - UploadWizard extension allows Cross-Site Scripting (XSS).This issue affects MediaWiki - UploadWizard extension: 1.45, 1.44, 1.43, 1.39.	6.1	More Details
CVE-2026-0670	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki - ProofreadPage Extension allows Cross-Site Scripting (XSS).This issue affects MediaWiki - ProofreadPage Extension: 1.45, 1.44, 1.43, 1.39.	6.1	More Details
CVE-2025-61676	October is a Content Management System (CMS) and web platform. Prior to versions 3.7.13 and 4.0.12, a cross-site scripting (XSS) vulnerabilities was identified in October CMS backend configuration forms. A user with the Customize Backend Styles permission could inject malicious HTML/JS into the stylesheet input at Styles from Branding & Appearance settings. A specially crafted input could break out of the intended <style> context, allowing arbitrary script execution across backend pages for all users. This issue has been patched in versions 3.7.13 and 4.0.12.	6.1	More Details
CVE-2025-14131	The WP Widget Changer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.2.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-12551	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins ListingHub listinghub allows Reflected XSS.This issue affects ListingHub: from n/a through 1.2.6.	6.1	More Details
CVE-2025-68892	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gopiplus@hotmail.com Scroll rss excerpt scroll-rss-excerpt allows Reflected XSS.This issue affects Scroll rss excerpt: from n/a through <= 5.0.	6.1	More Details
CVE-2019-25270	SOCA Access Control System 180612 contains a cross-site scripting vulnerability in the 'senddata' POST parameter of logged_page.php that allows attackers to inject malicious scripts. Attackers can exploit this weakness by sending crafted POST requests to execute arbitrary HTML and script code in a victim's browser session.	6.1	More Details
CVE-2025-68891	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Sutana WP App Bar wp-app-bar allows Reflected XSS.This issue affects WP App Bar: from n/a through <= 1.5.	6.1	More Details
CVE-2019-25277	FaceSentry Access Control System 6.4.8 contains a cross-site scripting vulnerability in the 'msg' parameter of pluginInstall.php that allows attackers to inject malicious scripts. Attackers can exploit the unvalidated input to execute arbitrary JavaScript in victim browsers, potentially stealing authentication credentials and conducting phishing attacks.	6.1	More Details
CVE-2025-68890	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hands01 e-shops e-shops-cart2 allows DOM-Based XSS.This issue affects e-shops: from n/a through <= 1.0.4.	6.1	More Details
CVE-2026-0514	Due to a Cross-Site Scripting (XSS) vulnerability in SAP Business Connector, an unauthenticated attacker could craft a malicious link. When an unsuspecting user clicks this link, the user may be redirected to a site controlled by the attacker. Successful exploitation could allow the attacker to access or modify information related to the webclient, impacting confidentiality and integrity, with no effect on availability.	6.1	More Details
CVE-2025-27004	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Famous - Responsive Image And Video Grid Gallery WordPress Plugin famous_grid_image_and_video_gallery allows Reflected XSS.This issue affects Famous - Responsive Image And Video Grid Gallery WordPress Plugin: from n/a through <= 1.4.	6.1	More Details
CVE-2019-	Yahei-PHP Prober 0.4.7 contains a remote HTML injection vulnerability that allows attackers to execute arbitrary HTML code through the 'speed' GET parameter. Attackers can inject malicious HTML code in the	6.1	More

25280	'speed' parameter of prober.php to trigger cross-site scripting in user browser sessions.		Details
CVE-2026-0618	Cross-site Scripting vulnerability in Devolutions PowerShell Universal.This issue affects Powershell Universal: before 4.5.6, before 5.6.13.	6.1	More Details
CVE-2023-54341	Webgrind 1.1 and before contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts via the file parameter in index.php. The application does not sufficiently encode user-controlled inputs, allowing attackers to execute arbitrary JavaScript in victim's browsers by crafting malicious URLs.	6.1	More Details
CVE-2019-25284	V-SOL GPON/EPON OLT Platform v2.03 contains multiple reflected cross-site scripting vulnerabilities due to improper input sanitization in various script parameters. Attackers can exploit these vulnerabilities by injecting malicious HTML and script code to execute arbitrary scripts in a victim's browser session.	6.1	More Details
CVE-2025-67932	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes Listeo Core listeo-core allows Reflected XSS.This issue affects Listeo Core: from n/a through < 2.0.19.	6.1	More Details
CVE-2025-67918	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WofficeIO Woffice woffice allows Reflected XSS.This issue affects Woffice: from n/a through <= 5.4.30.	6.1	More Details
CVE-2025-13893	The Lesson Plan Book plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13892	The MG AdvancedOptions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13519	The SVG Map Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on multiple AJAX actions including 'save_data', 'delete_data', and 'add_popup'. This makes it possible for unauthenticated attackers to update the plugin's settings, delete map data, and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-22695	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From 1.6.51 to 1.6.53, there is a heap buffer over-read in the libpng simplified API function png_image_finish_read when processing interlaced 16-bit PNGs with 8-bit output format and non-minimal row stride. This is a regression introduced by the fix for CVE-2025-65018. This vulnerability is fixed in 1.6.54.	6.1	More Details
CVE-2025-13369	The Premmerce WooCommerce Customers Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'money_spent_from', 'money_spent_to', 'registered_from', and 'registered_to' parameters in all versions up to, and including, 1.1.14 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13701	The Shabat Keeper plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the $_SERVER['PHP_SELF'] parameter in all versions up to, and including, 0.4.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-27002	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup CountDown With Image or Video Background countdown-with-background allows Reflected XSS.This issue affects CountDown With Image or Video Background: from n/a through <= 1.5.	6.1	More Details
CVE-2025-14128	The Stumble! for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2020-36919	WPForms 1.7.8 contains a cross-site scripting vulnerability in the slider import search feature and tab parameter. Attackers can inject malicious scripts through the ListTable.php endpoint to execute arbitrary JavaScript in victim's browser.	6.1	More Details
CVE-2023-	Zstore, now referred to as Zippy CRM, 6.5.4 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts through unvalidated input parameters. Attackers can submit crafted	6.1	More

53985	payloads in manual insertion points to execute arbitrary JavaScript code in victim's browser context.		Details
CVE-2026-22028	Preact, a lightweight web development framework, JSON serialization protection to prevent Virtual DOM elements from being constructed from arbitrary JSON. A regression introduced in Preact 10.26.5 caused this protection to be softened. In applications where values from JSON payloads are assumed to be strings and passed unmodified to Preact as children, a specially-crafted JSON payload could be constructed that would be incorrectly treated as a valid VNode. When this chain of failures occurs it can result in HTML injection, which can allow arbitrary script execution if not mitigated by CSP or other means. Applications using affected Preact versions are vulnerable if they meet all of the following conditions: first, pass unmodified, unsanitized values from user-modifiable data sources (APIs, databases, local storage, etc.) directly into the render tree; second assume these values are strings but the data source could return actual JavaScript objects instead of JSON strings; and third, the data source either fails to perform type sanitization AND blindly stores/returns raw objects interchangeably with strings, OR is compromised (e.g., poisoned local storage, filesystem, or database). Versions 10.26.10, 10.27.3, and 10.28.2 patch the issue. The patch versions restore the previous strict equality checks that prevent JSON-parsed objects from being treated as valid VNodes. Other mitigations are available for those who cannot immediately upgrade. Validate input types, cast or validate network data, sanitize external data, and use Content Security Policy (CSP).	6.1	More Details
CVE-2025-14127	The Testimonial Master plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 0.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-67916	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify Jobify jobify allows Reflected XSS.This issue affects Jobify: from n/a through <= 4.3.0.	6.1	More Details
CVE-2025-67922	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Restaurant grandrestaurant allows Reflected XSS.This issue affects Grand Restaurant: from n/a through < 7.0.9.	6.1	More Details
CVE-2025-14842	The Drag and Drop Multiple File Upload – Contact Form 7 plugin for WordPress is vulnerable to limited upload of files with a dangerous type in all versions up to, and including, 1.3.9.2. This is due to the plugin not blocking .phar and .svg files. This makes it possible for unauthenticated attackers to upload arbitrary .phar or .svg files containing malicious PHP or JavaScript code. Malicious PHP code can be used to achieve remote code execution on the server via direct file access, if the server is configured to execute .phar files as PHP. The upload of .svg files allows for Stored Cross-Site Scripting under certain circumstances.	6.1	More Details
CVE-2025-67927	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spencer Haws Link Whisper Free link-whisper allows Reflected XSS.This issue affects Link Whisper Free: from n/a through <= 0.8.8.	6.1	More Details
CVE-2023-54332	Jetpack 11.4 contains a cross-site scripting vulnerability in the contact form module that allows attackers to inject malicious scripts through the post_id parameter. Attackers can craft malicious URLs with script payloads to execute arbitrary JavaScript in victims' browsers when they interact with the contact form page.	6.1	More Details
CVE-2025-14875	The HBLPAY Payment Gateway for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘cusdata’ parameter in all versions up to, and including, 5.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2021-47750	YouPHPTube <= 7.8 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through the redirectUri parameter in the signup page. Attackers can craft special signup URLs with embedded script tags to execute arbitrary JavaScript in victims' browsers when they access the signup page.	6.1	More Details
CVE-2025-14130	The Post Like Dislike plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13504	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Real Estate Pro real-estate-pro allows Reflected XSS.This issue affects Real Estate Pro: from n/a through <= 2.1.4.	6.1	More Details
CVE-2025-67930	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vernon Systems Limited eHive Search ehive-search allows Reflected XSS.This issue affects eHive Search: from n/a through <= 2.5.0.	6.1	More Details
CVE-	The Top Position Google Finance plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 0.1.0 due to insufficient input		

2025-13895	sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-47331	Information disclosure while processing a firmware event.	6.1	More Details
CVE-2025-46644	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS2023 release versions 7.10.1.0 through 7.10.1.70, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	6.0	More Details
CVE-2025-13034	When using `CURLOPT_PINNEDPUBLICKEY` option with libcurl or `--pinnedpubkey` with the curl tool,curl should check the public key of the server certificate to verify the peer. This check was skipped in a certain condition that would then make curl allow the connection without performing the proper check, thus not noticing a possible impostor. To skip this check, the connection had to be done with QUIC with ngtcp2 built to use GnuTLS and the user had to explicitly disable the standard certificate verification.	5.9	More Details
CVE-2025-66560	Quarkus is a Cloud Native, (Linux) Container First framework for writing Java applications. Prior to versions 3.31.0, 3.27.2, and 3.20.5, a vulnerability exists in the HTTP layer of Quarkus REST related to response handling. When a response is being written, the framework waits for previously written response chunks to be fully transmitted before proceeding. If the client connection is dropped during this waiting period, the associated worker thread is never released and becomes permanently blocked. Under sustained or repeated occurrences, this can exhaust the available worker threads, leading to degraded performance, or complete unavailability of the application. This issue has been patched in versions 3.31.0, 3.27.2, and 3.20.5. A workaround involves implementing a health check that monitors the status and saturation of the worker thread pool to detect abnormal thread retention early.	5.9	More Details
CVE-2026-22798	hermes is an implementation of the HERMES workflow to automatize software publication with rich metadata. From 0.8.1 to before 0.9.1, hermes subcommands take arbitrary options under the -O argument. These have been logged in raw form. If users provide sensitive data such as API tokens (e.g., via hermes deposit -O invenio_rdm.auth_token SECRET), these are written to the log file in plain text, making them available to whoever can access the log file. This vulnerability is fixed in 0.9.1.	5.9	More Details
CVE-2026-22772	Fulcio is a certificate authority for issuing code signing certificates for an OpenID Connect (OIDC) identity. Prior to 1.8.5, Fulcio's metaRegex() function uses unanchored regex, allowing attackers to bypass MetaIssuer URL validation and trigger SSRF to arbitrary internal services. Since the SSRF only can trigger GET requests, the request cannot mutate state. The response from the GET request is not returned to the caller so data exfiltration is not possible. A malicious actor could attempt to probe an internal network through Blind SSRF. This vulnerability is fixed in 1.8.5.	5.8	More Details
CVE-2026-20026	Multiple Cisco products are affected by a vulnerability in the processing of DCE/RPC requests that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to leak sensitive information or to restart, resulting in an interruption of packet inspection. This vulnerability is due to an error in buffer handling logic when processing DCE/RPC requests, which can result in a buffer use-after-free read. An attacker could exploit this vulnerability by sending a large number of DCE/RPC requests through an established connection that is inspected by Snort 3. A successful exploit could allow the attacker to unexpectedly restart the Snort 3 Detection Engine, which could cause a denial of service (DoS).	5.8	More Details
CVE-2026-21859	Mailpit is an email testing tool and API for developers. Versions 1.28.0 and below have a Server-Side Request Forgery (SSRF) vulnerability in the /proxy endpoint, allowing attackers to make requests to internal network resources. The /proxy endpoint validates http:// and https:// schemes, but it does not block internal IP addresses, enabling attackers to access internal services and APIs. This vulnerability is limited to HTTP GET requests with minimal headers. The issue is fixed in version 1.28.1.	5.8	More Details
CVE-2025-68158	Authlib is a Python library which builds OAuth and OpenID Connect servers. In version 1.6.5 and prior, cache-backed state/request-token storage is not tied to the initiating user session, so CSRF is possible for any attacker that has a valid state (easily obtainable via an attacker-initiated authentication flow). When a cache is supplied to the OAuth client registry, FrameworkIntegration.set_state_data writes the entire state blob under _state_{app}_{state}, and get_state_data ignores the caller’s session altogether. This issue has been patched in version 1.6.6.	5.7	More Details
CVE-2025-14505	The ECDSA implementation of the Elliptic package generates incorrect signatures if an interim value of 'k' (as computed based on step 3.2 of RFC 6979 https://datatracker.ietf.org/doc/html/rfc6979) has leading zeros and is susceptible to cryptanalysis, which can lead to secret key exposure. This happens, because the byte-length of 'k' is incorrectly computed, resulting in its getting truncated during the computation. Legitimate transactions or communications will be broken as a result. Furthermore, due to the nature of the fault, attackers could–under certain conditions–derive the secret key, if they could get their hands on both a faulty signature generated by a vulnerable version of Elliptic and a correct signature for the same inputs. This issue	5.6	More Details

	affects all known versions of Elliptic (at the time of writing, versions less than or equal to 6.6.1).		
CVE-2026-21502	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to NULL pointer dereference via the XML tag parser. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-20819	Untrusted pointer dereference in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-21506	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to Null pointer dereference in CIccProfileXml::ParseBasic(), leading to denial of service. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-21505	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV has undefined behavior due to an invalid enum value. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-20823	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-20824	Protection mechanism failure in Windows Remote Assistance allows an unauthorized attacker to bypass a security feature locally.	5.5	More Details
CVE-2026-20805	Exposure of sensitive information to an unauthorized actor in Desktop Windows Manager allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-22188	Panda3D versions up to and including 1.10.16 deploy-stub contains a denial of service vulnerability due to unbounded stack allocation. The deploy-stub executable allocates argv_copy and argv_copy2 using alloca() based directly on the attacker-controlled argc value without validation. Supplying a large number of command-line arguments can exhaust stack space and propagate uninitialized stack memory into Python interpreter initialization, resulting in a reliable crash and undefined behavior.	5.5	More Details
CVE-2026-20827	Exposure of sensitive information to an unauthorized actor in Tablet Windows User Interface (TWINUI) Subsystem allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-20829	Out-of-bounds read in Windows TPM allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-68276	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. In 0.9-rc2 and earlier, an unprivileged local users can crash avahi-daemon (with wide-area disabled) by creating record browsers with the AVAHI_LOOKUP_USE_WIDE_AREA flag set via D-Bus. This can be done by either calling the RecordBrowserNew method directly or creating hostname/address/service resolvers/browsers that create those browsers internally themselves.	5.5	More Details
CVE-2026-20835	Out-of-bounds read in Capability Access Management Service (camsvc) allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-20833	Use of a broken or risky cryptographic algorithm in Windows Kerberos allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-20862	Exposure of sensitive information to an unauthorized actor in Windows Management Services allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-21500	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to stack overflow in the XML calculator macro expansion. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2025-9435	Zohocorp ManageEngine ADManager Plus versions below 7230 are vulnerable to Path Traversal in the User Management module	5.5	More Details
CVE-2026-21499	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to NULL pointer dereference via the XML parser. This issue has been patched in version 2.3.1.2.	5.5	More Details

CVE-2026-20838	Generation of error message containing sensitive information in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-20839	Improper access control in Windows Client-Side Caching (CSC) Service allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-21498	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to NULL pointer dereference via the XML calculator parser. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-21497	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to NULL pointer dereference via an unknown tag parser. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-21496	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to NULL pointer dereference via the signature parser. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-21495	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to division by zero in the TIFF Image Reader. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2026-21501	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.2, iccDEV is vulnerable to stack overflow in the calculator parser. This issue has been patched in version 2.3.1.2.	5.5	More Details
CVE-2025-62224	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an authorized attacker to perform spoofing over a network.	5.5	More Details
CVE-2026-21301	Substance3D - Modeler versions 1.22.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-20932	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-21288	Illustrator versions 29.8.3, 30.0 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21308	Substance3D - Designer versions 15.0.3 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21278	InDesign Desktop versions 21.0, 19.5.5 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-47330	Transient DOS while parsing video packets received from the video firmware.	5.5	More Details
CVE-2026-21300	Substance3D - Modeler versions 1.22.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21302	Substance3D - Modeler versions 1.22.4 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21303	Substance3D - Modeler versions 1.22.4 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE-2025-47369	Information disclosure when a weak hashed value is returned to userland code in response to a IOCTL call to obtain a session ID.	5.5	More Details
CVE-2026-20939	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-20937	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-46297	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.2. An app may be able to access protected files within an App Sandbox container.	5.5	More Details
CVE-2026-22231	OPEXUS eCASE Audit allows an authenticated attacker to save JavaScript as a comment within the Document Check Out functionality. The JavaScript is executed whenever another user views the Action History Log. Fixed in OPEXUS eCASE Platform 11.14.1.0.	5.5	More Details
CVE-2026-22232	OPEXUS eCASE Audit allows an authenticated attacker to save JavaScript in the "A or SIC Number" field within the Project Setup functionality. The JavaScript is executed whenever another user views the project. Fixed in OPEXUS eCASE Audit 11.14.2.0.	5.5	More Details
CVE-2026-22233	OPEXUS eCASE Audit allows an authenticated attacker to save JavaScript as a comment in the "Estimated Staff Hours" field. The JavaScript is executed whenever another user visits the Project Cost tab. Fixed in OPEXUS eCASE Audit 11.14.2.0.	5.5	More Details
CVE-2026-22703	Cosign provides code signing and transparency for containers and binaries. Prior to versions 2.6.2 and 3.0.4, Cosign bundle can be crafted to successfully verify an artifact even if the embedded Rekor entry does not reference the artifact's digest, signature or public key. When verifying a Rekor entry, Cosign verifies the Rekor entry signature, and also compares the artifact's digest, the user's public key from either a Fulcio certificate or provided by the user, and the artifact signature to the Rekor entry contents. Without these comparisons, Cosign would accept any response from Rekor as valid. A malicious actor that has compromised a user's identity or signing key could construct a valid Cosign bundle by including any arbitrary Rekor entry, thus preventing the user from being able to audit the signing event. This issue has been patched in versions 2.6.2 and 3.0.4.	5.5	More Details
CVE-2026-22587	Ideagen DevonWay contains a stored cross site scripting vulnerability. A remote, authenticated attacker could craft a payload in the 'Reports' page that executes when another user views the report. Fixed in 2.62.4 and 2.62 LTS.	5.5	More Details
CVE-2026-21639	A malicious actor in Wi-Fi range of the affected product could leverage a vulnerability in the airMAX Wireless Protocol to achieve a remote code execution (RCE) within the affected product. Affected Products: airMAX AC (Version 8.7.20 and earlier) airMAX M (Version 6.3.22 and earlier) airFiber AF60-XG (Version 1.2.2 and earlier) airFiber AF60 (Version 2.6.7 and earlier) Mitigation: Update your airMAX AC to Version 8.7.21 or later. Update your airMAX M to Version 6.3.24 or later. Update your airFiber AF60-XG to Version 1.2.3 or later. Update your airFiber AF60 to Version 2.6.8 or later.	5.4	More Details
CVE-2026-22517	Missing Authorization vulnerability in Passionate Brains GA4WP: Google Analytics for WordPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GA4WP: Google Analytics for WordPress: from n/a through 2.10.0.	5.4	More Details
CVE-2025-67282	In TIM BPM Suite/ TIM FLOW through 9.1.2 multiple Authorization Bypass vulnerabilities exists which allow a low privileged user to download password hashes of other user, access work items of other user, modify restricted content in workflows, modify the applications logo and manipulate the profile of other user.	5.4	More Details
CVE-2025-67281	In TIM BPM Suite/ TIM FLOW through 9.1.2 multiple SQL injection vulnerabilities exists which allow a low privileged and administrative user to access the database and its content.	5.4	More Details
CVE-2025-67280	In TIM BPM Suite/ TIM FLOW through 9.1.2 multiple Hibernate Query Language injection vulnerabilities exist which allow a low privileged user to extract passwords of other users and access sensitive data of another user.	5.4	More Details
CVE-2025-68718	KAYSUS KS-WR1200 routers with firmware 107 expose SSH and TELNET services on the LAN interface with hardcoded root credentials (root:12345678). The administrator cannot disable these services or change the hardcoded password. (Changing the management GUI password does not affect SSH/TELNET authentication.) Any LAN-adjacent attacker can trivially log in with root privileges.	5.4	More Details
CVE-2025-	The aBlocks – WordPress Gutenberg Blocks plugin for WordPress is vulnerable to unauthorized modification of data and disclosure of sensitive information due to missing capability checks on multiple AJAX actions in all versions up to, and including, 2.4.0. This makes it possible for authenticated attackers, with subscriber level	5.4	More

12449	access and above, to read plugin settings including block visibility, maintenance mode configuration, and third-party email marketing API keys, as well as read sensitive configuration data including API keys for email marketing services.		Details
CVE-2025-11246	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.4 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed an authenticated user with specific permissions to remove all project runners from unrelated projects by manipulating GraphQL runner associations.	5.4	More Details
CVE-2025-61550	Cross-Site Scripting (XSS) is present on the ctl00_Content01_fieldValue parameters on the /psp/appNet/TemplateOrder/TemplatePreview.aspx endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34. User-supplied input is stored and later rendered in HTML pages without proper output encoding or sanitization. This allows attackers to persistently inject arbitrary JavaScript that executes in the context of other users' sessions	5.4	More Details
CVE-2021-41074	A CSRF issue in index.php in QloApps hotel eCommerce 1.5.1 allows an attacker to change the admin's email address via a crafted HTML document.	5.4	More Details
CVE-2025-14718	The Schedule Post Changes With PublishPress Future plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.9.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Contributor-level access and above, to create, update, delete, and publish malicious workflows that may automatically delete any post upon publication or update, including posts created by administrators.	5.4	More Details
CVE-2025-66939	Cross Site Scripting vulnerability in 66biolinks by AltumCode v.61.0.1 allows an attacker to execute arbitrary code via a crafted favicon file	5.4	More Details
CVE-2026-22789	WebErpMesv2 is a Resource Management and Manufacturing execution system Web for industry. Prior to 1.19, WebErpMesv2 contains a file upload validation bypass vulnerability in multiple controllers that allows authenticated users to upload arbitrary files, including PHP scripts, leading to Remote Code Execution (RCE). This vulnerability is identical in nature to CVE-2025-52130 but exists in different code locations that were not addressed by the original fix. This vulnerability is fixed in 1.19.	5.4	More Details
CVE-2026-21691	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of International Color Consortium (ICC) color management profiles. Versions prior to 2.3.1.2 have a Type Confusion vulnerability in `CIccTag:IsTypeCompressed()`. This vulnerability affects users of the iccDEV library who process ICC color profiles. Version 2.3.1.2 contains a patch. No known workarounds are available.	5.4	More Details
CVE-2026-22490	Missing Authorization vulnerability in niklaslindemann Bulk Landing Page Creator for WordPress LPagery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Bulk Landing Page Creator for WordPress LPagery: from n/a through 2.4.9.	5.4	More Details
CVE-2026-22253	Soft Serve is a self-hostable Git server for the command line. Prior to version 0.11.2, an authorization bypass in the LFS lock deletion endpoint allows any authenticated user with repository write access to delete locks owned by other users by setting the force flag. The vulnerable code path processes force deletions before retrieving user context, bypassing ownership validation entirely. This issue has been patched in version 0.11.2.	5.4	More Details
CVE-2025-14001	The WP Duplicate Page plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on the 'duplicateBulkHandle' and 'duplicateBulkHandleHPOS' functions in all versions up to, and including, 1.8. This makes it possible for authenticated attackers, with Contributor-level access and above, to duplicate arbitrary posts, pages, and WooCommerce HPOS orders even when their role is explicitly excluded from the plugin's "Allowed User Roles" setting, potentially exposing sensitive information and allowing duplicate fulfillment of WooCommerce orders.	5.4	More Details
CVE-2025-14802	The LearnPress – WordPress LMS Plugin for WordPress is vulnerable to unauthorized file deletion in versions up to, and including, 4.3.2.2 via the /wp-json/lp/v1/material/{file_id} REST API endpoint. This is due to a parameter mismatch between the DELETE operation and authorization check, where the endpoint uses file_id from the URL path but the permission callback validates item_id from the request body. This makes it possible for authenticated attackers, with teacher-level access, to delete arbitrary lesson material files uploaded by other teachers via sending a DELETE request with their own item_id (to pass authorization) while targeting another teacher's file_id.	5.4	More Details
CVE-2025-22725	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in loopus WP Virtual Assistant VirtualAssistant allows Stored XSS.This issue affects WP Virtual Assistant: from n/a through <= 3.0.	5.4	More Details
CVE-2025-14976	The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.4.8. This is due to missing or incorrect nonce validation on the 'process_row_actions' function with the 'delete' action. This makes it possible for unauthenticated attackers	5.4	More Details

	to delete arbitrary post via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2026-20958	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to disclose information over a network.	5.4	More Details
CVE-2025-61782	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to version 6.8.3, an open redirect vulnerability exists in the OpenCTI platform's SAML authentication endpoint (/auth/saml/callback). By manipulating the RelayState parameter, an attacker can force the server to issue a 302 redirect to any external URL, enabling phishing, credential theft, and arbitrary site redirection. This issue has been patched in version 6.8.3.	5.4	More Details
CVE-2025-69169	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Noor Alam Easy Media Download easy-media-download allows Reflection Injection.This issue affects Easy Media Download: from n/a through <= 1.1.11.	5.4	More Details
CVE-2025-68875	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jcaruso001 Flaming Password Reset flaming-password-reset allows Stored XSS.This issue affects Flaming Password Reset: from n/a through <= 1.0.3.	5.4	More Details
CVE-2023-7333	A weakness has been identified in bluelabsio records-mover up to 1.5.4. The affected element is an unknown function of the component Table Object Handler. This manipulation causes sql injection. The attack needs to be launched locally. Upgrading to version 1.6.0 is sufficient to fix this issue. Patch name: 3f8383aa89f45d861ca081e3e9fd2cc9d0b5dfaa. You should upgrade the affected component.	5.3	More Details
CVE-2026-0731	A vulnerability has been found in TOTOLINK WA1200 5.9c.2914. The impacted element is an unknown function of the file cstecgi.cgi of the component HTTP Request Handler. The manipulation leads to null pointer dereference. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2025-12648	The WP-Members Membership Plugin for WordPress is vulnerable to unauthorized file access in versions up to, and including, 3.5.4.4. This is due to storing user-uploaded files in predictable directories (wp-content/uploads/wpmembers/user_files/<user_id>/) without implementing proper access controls beyond basic directory listing protection (.htaccess with Options -Indexes). This makes it possible for unauthenticated attackers to directly access and download sensitive documents uploaded by site users via direct URL access, granted they can guess or enumerate user IDs and filenames.	5.3	More Details
CVE-2026-0887	Clickjacking issue, information disclosure in the PDF Viewer component. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	5.3	More Details
CVE-2026-20027	Multiple Cisco products are affected by a vulnerability in the processing of DCE/RPC requests that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to leak sensitive information or to restart, resulting in an interruption of packet inspection. This vulnerability is due to an error in buffer handling logic when processing DCE/RPC requests, which can result in a buffer out-of-bounds read. An attacker could exploit this vulnerability by sending a large number of DCE/RPC requests through an established connection that is inspected by Snort 3. A successful exploit could allow the attacker to obtain sensitive information in the Snort 3 data stream.	5.3	More Details
CVE-2026-21851	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. In versions up to and including 1.5.1, a Path Traversal (Zip Slip) vulnerability exists in MONAI's `_download_from_ngc_private()` function. The function uses `zipfile.ZipFile.extractall()` without path validation, while other similar download functions in the same codebase properly use the existing `safe_extract_member()` function. Commit 4014c8475626f20f158921ae0cf98ed259ae4d59 fixes this issue.	5.3	More Details
CVE-2026-22701	filelock is a platform-independent file lock for Python. Prior to version 3.20.3, a TOCTOU race condition vulnerability exists in the SoftFileLock implementation of the filelock package. An attacker with local filesystem access and permission to create symlinks can exploit a race condition between the permission validation and file creation to cause lock operations to fail or behave unexpectedly. The vulnerability occurs in the _acquire() method between raise_on_not_writable_file() (permission check) and os.open() (file creation). During this race window, an attacker can create a symlink at the lock file path, potentially causing the lock to operate on an unintended target file or leading to denial of service. This issue has been patched in version 3.20.3.	5.3	More Details
CVE-2026-0707	A flaw was found in Keycloak. The Keycloak Authorization header parser is overly permissive regarding the formatting of the "Bearer" authentication scheme. It accepts non-standard characters (such as tabs) as separators and tolerates case variations that deviate from RFC 6750 specifications.	5.3	More Details
CVE-2025-14948	The miniOrange OTP Verification and SMS Notification for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `enable_wc_sms_notification` AJAX action in all versions up to, and including, 4.3.8. This makes it possible for unauthenticated attackers to	5.3	More Details

	enable or disable SMS notification settings for WooCommerce orders.		
CVE-2025-13419	The Guest posting / Frontend Posting / Front Editor – WP Front User Submit plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the '/wp-json/bfe/v1/revert' REST API endpoint in all versions up to, and including, 5.0.0. This makes it possible for unauthenticated attackers to delete arbitrary media attachments.	5.3	More Details
CVE-2026-0888	Information disclosure in the XML component. This vulnerability affects Firefox < 147.	5.3	More Details
CVE-2025-13694	The AA Block Country plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 1.0.1. This is due to the plugin trusting user-supplied headers such as HTTP_X_FORWARDED_FOR to determine the client's IP address without proper validation or considering if the server is behind a trusted proxy. This makes it possible for unauthenticated attackers to bypass IP-based access restrictions by spoofing their IP address via the X-Forwarded-For header.	5.3	More Details
CVE-2026-0886	Incorrect boundary conditions in the Graphics component. This vulnerability affects Firefox < 147, Firefox ESR < 115.32, and Firefox ESR < 140.7.	5.3	More Details
CVE-2026-0853	Certain NVR models developed by A-Plus Video Technologies has a Sensitive Data Exposure vulnerability, allowing unauthenticated remote attackers to access the debug page and obtain device status information.	5.3	More Details
CVE-2025-13529	The Unify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'init' action in all versions up to, and including, 3.4.9. This makes it possible for unauthenticated attackers to delete specific plugin options via the 'unify_plugin_downgrade' parameter.	5.3	More Details
CVE-2025-31051	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in EngoTheme Plant - Gardening & Houseplants WordPress Theme allows Retrieve Embedded Sensitive Data.This issue affects Plant - Gardening & Houseplants WordPress Theme: from n/a through 1.0.0.	5.3	More Details
CVE-2026-20927	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB Server allows an authorized attacker to deny service over a network.	5.3	More Details
CVE-2026-0883	Information disclosure in the Networking component. This vulnerability affects Firefox < 147 and Firefox ESR < 140.7.	5.3	More Details
CVE-2019-25259	Leica Geosystems GR10/GR25/GR30/GR50 GNSS 4.30.063 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions without request validation. Attackers can trick logged-in users into executing unauthorized actions by crafting malicious web pages that submit requests to the application.	5.3	More Details
CVE-2026-0831	The Templately plugin for WordPress is vulnerable to Arbitrary File Write in all versions up to, and including, 3.4.8. This is due to inadequate input validation in the `save_template_to_file()` function where user-controlled parameters like `session_id`, `content_id`, and `ai_page_ids` are used to construct file paths without proper sanitization. This makes it possible for unauthenticated attackers to write arbitrary `.ai.json` files to locations within the uploads directory.	5.3	More Details
CVE-2026-21880	Kanboard is project management software focused on Kanban methodology. Versions 1.2.48 and below have an LDAP Injection vulnerability in the LDAP authentication mechanism. User-supplied input is directly substituted into LDAP search filters without proper sanitization, allowing attackers to enumerate all LDAP users, discover sensitive user attributes, and perform targeted attacks against specific accounts. This issue is fixed in version 1.2.49.	5.3	More Details
CVE-2026-22486	Missing Authorization vulnerability in Hakob Re Gallery & Responsive Photo Gallery Plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Re Gallery & Responsive Photo Gallery Plugin: from n/a through 1.17.18.	5.3	More Details
CVE-2025-14524	When an OAuth2 bearer token is used for an HTTP(S) transfer, and that transfer performs a cross-protocol redirect to a second URL that uses an IMAP, LDAP, POP3 or SMTP scheme, curl might wrongly pass on the bearer token to the new target host.	5.3	More Details
CVE-2026-22488	Missing Authorization vulnerability in IdeaBox Creations Dashboard Welcome for Beaver Builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Dashboard Welcome for Beaver Builder: from n/a through 1.0.8.	5.3	More Details
CVE-2025-	The EventPrime - Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.2.7.0 via the REST API. This makes it possible for unauthenticated attackers to extract sensitive booking data including user names, email addresses, ticket	5.3	More

14507	details, payment information, and order keys when the API is enabled by an administrator. The vulnerability was partially patched in version 4.2.7.0.		Details
CVE-2019-25290	Smartliving SmartLAN/G/SI <=6.x contains an unauthenticated server-side request forgery vulnerability in the GetImage functionality through the 'host' parameter. Attackers can exploit the onvif.cgi endpoint by specifying external domains to bypass firewalls and perform network enumeration through arbitrary HTTP requests.	5.3	More Details
CVE-2025-13496	The Moosend Landing Pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the moosend_landings_auth_get function in all versions up to, and including, 1.1.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the 'moosend_landing_api_key' option value.	5.3	More Details
CVE-2025-15079	When doing SSH-based transfers using either SCP or SFTP, and setting the known_hosts file, libcurl could still mistakenly accept connecting to hosts *not present* in the specified file if they were added as recognized in the libssh *global* known_hosts file.	5.3	More Details
CVE-2025-67813	Quest KACE Desktop Authority through 11.3.1 has Insecure Permissions on the Named Pipes used for inter-process communication	5.3	More Details
CVE-2025-13717	The Contact Form vCard Generator plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'wp_gvccf_check_download_request' function in all versions up to, and including, 2.4. This makes it possible for unauthenticated attackers to export sensitive Contact Form 7 submission data via the 'wp-gvc-cf-download-id' parameter, including names, phone numbers, email addresses, and messages.	5.3	More Details
CVE-2026-21892	Parsl is a Python parallel scripting library. A SQL Injection vulnerability exists in the parsl-visualize component of versions prior to 2026.01.05. The application constructs SQL queries using unsafe string formatting (Python % operator) with user-supplied input (workflow_id) directly from URL routes. This allows an unauthenticated attacker with access to the visualization dashboard to inject arbitrary SQL commands, potentially leading to data exfiltration or denial of service against the monitoring database. Version 2026.01.05 fixes the issue.	5.3	More Details
CVE-2025-37178	Multiple out-of-bounds read vulnerabilities were identified in a system component responsible for handling certain data buffers. Due to insufficient validation of maximum buffer size values, the process may attempt to read beyond the intended memory region. Under specific conditions, this can result in a crash of the affected process and a potential denial-of-service of the compromised process.	5.3	More Details
CVE-2025-37179	Multiple out-of-bounds read vulnerabilities were identified in a system component responsible for handling certain data buffers. Due to insufficient validation of maximum buffer size values, the process may attempt to read beyond the intended memory region. Under specific conditions, this can result in a crash of the affected process and a potential denial-of-service of the compromised process.	5.3	More Details
CVE-2025-14460	The Piraeus Bank WooCommerce Payment Gateway plugin for WordPress is vulnerable to unauthorized order status modification in all versions up to, and including, 3.1.4. This is due to missing authorization checks on the payment callback endpoint handler when processing the 'fail' callback from the payment gateway. This makes it possible for unauthenticated attackers to change any order's status to 'failed' via the publicly accessible WooCommerce API endpoint by providing only the order ID (MerchantReference parameter), which can be easily enumerated as order IDs are sequential integers. This can cause significant business disruption including canceled shipments, inventory issues, and loss of revenue.	5.3	More Details
CVE-2025-14370	The Quote Comments plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.0.0. This is due to missing authorization checks in the quotecomments_add_admin function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary plugin options via the 'action' parameter.	5.3	More Details
CVE-2025-14352	The Awesome Hotel Booking plugin for WordPress is vulnerable to unauthorized modification of data due to incorrect authorization in the room-single.php shortcode handler in all versions up to, and including, 1.0. This is due to the plugin relying solely on nonce verification without capability checks. This makes it possible for unauthenticated attackers to modify arbitrary booking records by obtaining a nonce from the public booking form.	5.3	More Details
CVE-2026-0817	Missing Authorization vulnerability in Wikimedia Foundation MediaWiki - CampaignEvents extension allows Privilege Abuse.This issue affects MediaWiki - CampaignEvents extension: 1.45, 1.44, 1.43, 1.39.	5.3	More Details
CVE-2025-68949	n8n is an open source workflow automation platform. From 1.36.0 to before 2.2.0, the Webhook node’s IP whitelist validation performed partial string matching instead of exact IP comparison. As a result, an incoming request could be accepted if the source IP address merely contained the configured whitelist entry as a substring. This issue affected instances where workflow editors relied on IP-based access controls to restrict webhook access. Both IPv4 and IPv6 addresses were impacted. An attacker with a non-whitelisted IP could	5.3	More Details

	bypass restrictions if their IP shared a partial prefix with a trusted address, undermining the intended security boundary. This vulnerability is fixed in 2.2.0.		
CVE-2026-21874	NiceGUI is a Python-based UI framework. From versions v2.10.0 to 3.4.1, an unauthenticated attacker can exhaust Redis connections by repeatedly opening and closing browser tabs on any NiceGUI application using Redis-backed storage. Connections are never released, leading to service degradation when Redis hits its connection limit. NiceGUI continues accepting new connections - errors are logged but the app stays up with broken storage functionality. This issue has been patched in version 3.5.0.	5.3	More Details
CVE-2025-67279	An issue in TIM Solution GmbH TIM BPM Suite & TIM FLOW before v.9.1.2 allows a remote attacker to escalate privileges via the application stores password hashes in MD5 format	5.3	More Details
CVE-2026-0676	Missing Authorization vulnerability in G5Theme Zorka zorka allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Zorka: from n/a through <= 1.5.7.	5.3	More Details
CVE-2026-22251	wlc is a Weblate command-line client using Weblate's REST API. Prior to 1.17.0, wlc supported providing unscoped API keys in the setting. This practice was discouraged for years, but the code was never removed. This might cause the API key to be leaked to different servers.	5.3	More Details
CVE-2025-13722	The Fluent Forms – Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 6.1.7. This is due to missing capability checks on the `fluentform_ai_create_form` AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary forms via the publicly exposed AI builder.	5.3	More Details
CVE-2025-14819	When doing TLS related transfers with reused easy or multi handles and altering the `CURLSSLOPT_NO_PARTIALCHAIN` option, libcurl could accidentally reuse a CA store cached in memory for which the partial chain option was reversed. Contrary to the user's wishes and expectations. This could make libcurl find and accept a trust chain that it otherwise would not.	5.3	More Details
CVE-2025-14782	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.49.1 via the 'listen_for_csv_export' function. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with access to the Forminator dashboard, to export sensitive form submission data including personally identifiable information.	5.3	More Details
CVE-2025-14720	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to unauthorized access due to missing capability checks on multiple AJAX actions in all versions up to, and including, 1.2.38. This makes it possible for unauthenticated attackers to mark payments as refunded, trigger sending of queued notifications (emails/SMS/WhatsApp), and access debug information among other things.	5.3	More Details
CVE-2025-65090	XWiki Full Calendar Macro displays objects from the wiki on the calendar. Prior to version 2.4.6, users with the rights to view the Calendar.JSONService page (including guest users) can exploit the data leak vulnerability by accessing database info, with the exception of passwords. This issue has been patched in version 2.4.6.	5.3	More Details
CVE-2025-14886	The Japanized for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `order` REST API endpoint in all versions up to, and including, 2.7.17. This makes it possible for unauthenticated attackers to mark any WooCommerce order as processed/completed.	5.3	More Details
CVE-2026-22041	Logging Redactor is a Python library designed to redact sensitive data in logs based on regex patterns and / or dictionary keys. Prior to version 0.0.6, non-string types are converted into string types, leading to type errors in %d conversions. The problem has been patched in version 0.0.6. No known workarounds are available.	5.3	More Details
CVE-2025-14146	The Booking Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 10.14.10 via the `WPBC_FLEXTIMELINE_NAV` AJAX action. This is due to the nonce verification being conditionally disabled by default (`booking_is_nonce_at_front_end` option is `'Off'` by default). When the `booking_is_show_popover_in_timeline_front_end` option is enabled (which is the default in demo installations and can be enabled by administrators), it is possible for unauthenticated attackers to extract sensitive booking data including customer names, email addresses, phone numbers, and booking details.	5.3	More Details
CVE-2026-20973	Out-of-bounds read in libimagecodec.quram.so prior to SMR Jan-2026 Release 1 allows remote attacker to access out-of-bounds memory.	5.3	More Details
CVE-2026-	HarfBuzz is a text shaping engine. Prior to version 12.3.0, a null pointer dereference vulnerability exists in the SubtableUnicodesCache::create function located in src/hb-ot-cmap-table.hh. The function fails to check if hb_malloc returns NULL before using placement new to construct an object at the returned pointer address. When hb_malloc fails to allocate memory (which can occur in low-memory conditions or when using custom	5.3	More Details

22693	allocators that simulate allocation failures), it returns NULL. The code then attempts to call the constructor on this null pointer using placement new syntax, resulting in undefined behavior and a Segmentation Fault. This issue has been patched in version 12.3.0.		
CVE-2025-14574	The weDocs plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.1.15 via the `/wp-json/wp/v2/docs/settings` REST API endpoint. This makes it possible for unauthenticated attackers to extract sensitive data including third party services API keys.	5.3	More Details
CVE-2026-0668	Inefficient Regular Expression Complexity vulnerability in Wikimedia Foundation MediaWiki - VisualData Extension allows Regular Expression Exponential Blowup.This issue affects MediaWiki - VisualData Extension: 1.45.	5.3	More Details
CVE-2026-0495	SAP Fiori App Intercompany Balance Reconciliation allows an attacker with high privileges to send uploaded files to arbitrary emails which could enable effective phishing campaigns. This has low impact on confidentiality, integrity and availability of the application.	5.1	More Details
CVE-2025-67090	The LuCI web interface on GI Inet GL.Inet AX1800 Version 4.6.4 & 4.6.8 are vulnerable. Fix available in version 4.8.2 GL.Inet AX1800 Version 4.6.4 & 4.6.8 lacks rate limiting or account lockout mechanisms on the authentication endpoint (`/cgi-bin/luci`). An unauthenticated attacker on the local network can perform unlimited password attempts against the admin interface.	5.1	More Details
CVE-2024-14020	A weakness has been identified in carboneio carbone up to fbcd349077ad0e8748be73eab2a82ea92b6f8a7e. This impacts an unknown function of the file lib/input.js of the component Formatter Handler. Executing a manipulation can lead to improperly controlled modification of object prototype attributes. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is said to be difficult. Upgrading to version 3.5.6 will fix this issue. This patch is called 04f9feb24bfca23567706392f9ad2c53bbe4134e. You should upgrade the affected component. A successful exploitation can "only occur if the parent NodeJS application has the same security issue".	5.0	More Details
CVE-2025-49335	Server-Side Request Forgery (SSRF) vulnerability in minnur External Media allows Server Side Request Forgery.This issue affects External Media: from n/a through 1.0.36.	4.9	More Details
CVE-2026-20029	A vulnerability in the licensing features of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, remote attacker with administrative privileges to gain access to sensitive information. This vulnerability is due to improper parsing of XML that is processed by the web-based management interface of Cisco ISE and Cisco ISE-PIC. An attacker could exploit this vulnerability by uploading a malicious file to the application. A successful exploit could allow the attacker to read arbitrary files from the underlying operating system that could include sensitive data that should otherwise be inaccessible even to administrators. To exploit this vulnerability, the attacker must have valid administrative credentials.	4.9	More Details
CVE-2025-62327	In HCL DevOps Deploy 8.1.2.0 through 8.1.2.3, a user with LLM configuration privileges may be able to recover a credential previously saved for performing authenticated LLM Queries.	4.9	More Details
CVE-2026-22242	CoreShop is a Pimcore enhanced eCommerce solution. Prior to version 4.1.8, a blind SQL injection vulnerability exists in the application that allows an authenticated administrator-level user to extract database contents using boolean-based or time-based techniques. The database account used by the application is read-only and non-DBA, limiting impact to confidential data disclosure only. No data modification or service disruption is possible. This issue has been patched in version 4.1.8.	4.9	More Details
CVE-2025-14719	The Relevanssi WordPress plugin before 4.26.0, Relevanssi Premium WordPress plugin before 2.29.0 do not sanitize and escape a parameter before using it in a SQL statement, allowing contributor and above roles to perform SQL injection attacks	4.9	More Details
CVE-2026-0716	A flaw was found in libsoup’s WebSocket frame processing when handling incoming messages. If a non-default configuration is used where the maximum incoming payload size is unset, the library may read memory outside the intended bounds. This can cause unintended memory exposure or a crash. Applications using libsoup’s WebSocket support with this configuration may be impacted.	4.8	More Details
CVE-2025-14579	The Quiz Maker WordPress plugin before 6.7.0.89 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2025-15495	A vulnerability was found in BiggiDroid Simple PHP CMS 1.0. This impacts an unknown function of the file /admin/editsite.php. The manipulation of the argument image results in unrestricted upload. The attack can be launched 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-2026-	A vulnerability was determined in code-projects Intern Membership Management System 1.0. Impacted is an unknown function of the file /admin/delete_activity.php. Executing a manipulation of the argument activity_id	4.7	More

0850	can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.		Details
CVE-2026-21879	Kanboard is project management software focused on Kanban methodology. Versions 1.2.48 and below are vulnerable to an Open Redirect attack that allows malicious actors to redirect authenticated users to attacker-controlled websites. By crafting URLs such as //evil.com, attackers can bypass the filter_var($url, FILTER_VALIDATE_URL) validation check. This vulnerability could be exploited to conduct phishing attacks, steal user credentials, or distribute malware. The issue is fixed in version 1.2.49.	4.7	More Details
CVE-2025-68947	NSecsoft 'NSecKrnl' is a Windows driver that allows a local, authenticated attacker to terminate processes owned by other users, including SYSTEM and Protected Processes by issuing crafted IOCTL requests to the driver.	4.7	More Details
CVE-2026-0729	A vulnerability was detected in code-projects Intern Membership Management System 1.0. Impacted is an unknown function of the file /intern/admin/add_activity.php. Performing a manipulation of the argument Title results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	4.7	More Details
CVE-2025-12540	The ShareThis Dashboard for Google Analytics plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.2.4. This is due to the Google Analytics client_ID and client_secret being stored in plaintext in the publicly visible plugin source. This can allow unauthenticated attackers to craft a link to the sharethis.com server, which will share an authorization token for Google Analytics with a malicious website, if the attacker can trick an administrator logged into the website and Google Analytics to click the link.	4.7	More Details
CVE-2026-0728	A security vulnerability has been detected in code-projects Intern Membership Management System 1.0. This issue affects some unknown processing of the file /intern/admin/delete_admin.php. Such manipulation of the argument admin_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2026-0513	Due to an Open Redirect Vulnerability in SAP Supplier Relationship Management (SICF Handler in SRM Catalog), an unauthenticated attacker could craft a malicious URL that, if accessed by a victim, redirects them to an attacker-controlled site.This causes low impact on integrity of the application. Confidentiality and availability are not impacted.	4.7	More Details
CVE-2026-0649	A security vulnerability has been detected in invoiceninja up to 5.12.38. The affected element is the function copy of the file /app/Jobs/Util/Import.php of the component Migration Import. The manipulation of the argument company_logo leads to server-side request forgery. It is possible to initiate 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-2026-21899	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, in base64urlDecode, padding-stripping dereferences input[inputLen - 1] before checking that inputLen > 0 or that input != NULL. For inputLen == 0, this becomes an OOB read at input[-1], potentially crashing the process. If input == NULL and inputLen == 0, it dereferences NULL - 1. This issue has been patched in version 1.4.3.	4.7	More Details
CVE-2026-0697	A flaw has been found in code-projects Intern Membership Management System 1.0. The impacted element is an unknown function of the file /intern/admin/edit_admin.php. This manipulation of the argument admin_id causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2026-0701	A vulnerability was identified in code-projects Intern Membership Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /intern/admin/add_admin.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-0699	A vulnerability was found in code-projects Intern Membership Management System 1.0. This impacts an unknown function of the file /intern/admin/edit_activity.php. Performing a manipulation of the argument activity_id results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	4.7	More Details
CVE-2026-0698	A vulnerability has been found in code-projects Intern Membership Management System 1.0. This affects an unknown function of the file /intern/admin/edit_students.php. Such manipulation of the argument admin_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2026-20959	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-	Absolute path traversal in Windows Shell allows an unauthorized attacker to perform spoofing with a physical	4.6	More

20834	attack.		Details
CVE-2026-20828	Out-of-bounds read in Windows Internet Connection Sharing (ICS) allows an unauthorized attacker to disclose information with a physical attack.	4.6	More Details
CVE-2026-22702	virtualenv is a tool for creating isolated virtual python environments. Prior to version 20.36.1, TOCTOU (Time-of-Check-Time-of-Use) vulnerabilities in virtualenv allow local attackers to perform symlink-based attacks on directory creation operations. An attacker with local access can exploit a race condition between directory existence checks and creation to redirect virtualenv's app_data and lock file operations to attacker-controlled locations. This issue has been patched in version 20.36.1.	4.5	More Details
CVE-2025-14888	The Simple User Meta Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user meta value field in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-22809	tarteaucitron.js is a compliant and accessible cookie banner. Prior to 1.29.0, a Regular Expression Denial of Service (ReDoS) vulnerability was identified in tarteaucitron.js in the handling of the issuu_id parameter. This vulnerability is fixed in 1.29.0.	4.4	More Details
CVE-2025-14057	The Multi-column Tag Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 17.0.39 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-13974	The Email Customizer for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email template content in all versions up to, and including, 2.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in email templates that will execute when customers view transactional emails. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-20825	Improper access control in Windows Hyper-V allows an authorized attacker to disclose information locally.	4.4	More Details
CVE-2025-14028	The Contact Us Simple Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2025-14887	The twinklesmtp – Email Service Provider For WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin's sender settings in all versions up to, and including, 1.03 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-20962	Use of uninitialized resource in Dynamic Root of Trust for Measurement (DRTM) allows an authorized attacker to disclose information locally.	4.4	More Details
CVE-2025-15000	The Page Keys plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘page_key’ parameter in all versions up to, and including, 1.3.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-14792	The Key Figures plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the kf_field_figure_default_color_render function in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-0674	Missing Authorization vulnerability in Campaign Monitor Campaign Monitor for WordPress forms-for-campaign-monitor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Campaign Monitor for WordPress: from n/a through <= 2.9.0.	4.3	More Details
CVE-	The WP Table Builder – Drag & Drop Table Builder plugin for WordPress is vulnerable to unauthorized		

2025-13753	modification of data due to an incorrect authorization check on the save_table() function in all versions up to, and including, 2.0.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create new wptb-table posts.	4.3	More Details
CVE-2025-14904	The Newsletter Email Subscribe plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4. This is due to incorrect nonce validation on the nels_settings_page function. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-14999	The Latest Tabs plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5. This is due to missing or incorrect nonce validation on the settings update handler in admin-page.php. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-14845	The NS IE Compatibility Fixer plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in all versions up to, and including, 2.1.5. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-14077	The Simcast plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the settingsPage function. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-46299	A memory initialization issue was addressed with improved memory handling. This issue is fixed in tvOS 26.2, Safari 26.2, watchOS 26.2, visionOS 26.2, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2. Processing maliciously crafted web content may disclose internal states of the app.	4.3	More Details
CVE-2025-46286	A logic issue was addressed with improved validation. This issue is fixed in iOS 26.2 and iPadOS 26.2. Restoring from a backup may prevent passcode from being required immediately after Face ID enrollment.	4.3	More Details
CVE-2025-13628	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized modification and deletion of data due to a missing capability check on the 'bulk_action_handler' and 'coupon_permanent_delete' functions in all versions up to, and including, 3.9.3. This makes it possible for authenticated attackers, with subscriber level access and above, to delete, activate, deactivate, or trash arbitrary coupons.	4.3	More Details
CVE-2025-13934	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized course enrollment in all versions up to, and including, 3.9.3. This is due to a missing capability check and purchasability validation in the `course_enrollment()` AJAX handler. This makes it possible for authenticated attackers, with subscriber level access and above, to enroll themselves in any course without going through the proper purchase flow.	4.3	More Details
CVE-2025-69344	Missing Authorization vulnerability in ThemeHunk Oneline Lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Oneline Lite: from n/a through 6.6.	4.3	More Details
CVE-2025-13935	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized course completion in all versions up to, and including, 3.9.2. This is due to missing enrollment verification in the 'mark_course_complete' function. This makes it possible for authenticated attackers, with subscriber level access and above, to mark any course as completed.	4.3	More Details
CVE-2025-14468	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.9. This is due to inverted nonce verification logic in the amp_theme_ajaxcomments AJAX handler, which rejects requests with VALID nonces and accepts requests with MISSING or INVALID nonces. This makes it possible for unauthenticated attackers to submit comments on behalf of logged-in users via a forged request granted they can trick a user into performing an action such as clicking on a link, and the plugin's template mode is enabled.	4.3	More Details
CVE-2026-22032	Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 11.14.0, an open redirect vulnerability exists in the Directus SAML authentication callback endpoint. During SAML authentication, the `RelayState` parameter is intended to preserve the user's original destination. However, while the login initiation flow validates redirect targets against allowed domains, this validation is not applied to the callback endpoint. This allows an attacker to craft a malicious authentication request that redirects users to an arbitrary external URL upon completion. The vulnerability is present in both the success and error handling paths of the callback. This vulnerability can be exploited without authentication. Version 11.14.0 contains a patch.	4.3	More Details
CVE-2025-	The Sticky Action Buttons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the sabs_options_page_form_submit() function. This makes it possible for unauthenticated attackers to update	4.3	More Details

14465	plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		
CVE-2025-68658	Open Source Point of Sale (opensourcepos) is a web based point of sale application written in PHP using CodeIgniter framework. opensourcepos 3.4.0 and 3.4.1 has a stored XSS vulnerability exists in the Configuration (Information) functionality. An authenticated user with the permission “Configuration: Change OSPOS's Configuration” can inject a malicious JavaScript payload into the Company Name field when updating Information in Configuration. The malicious payload is stored and later triggered when a user accesses /sales/complete. First select Sales, and choose New Item to create an item, then click on Completed . Due to insufficient input validation and output encoding, the payload is rendered and executed in the user’s browser, resulting in a stored XSS vulnerability. This vulnerability is fixed in 3.4.2.	4.3	More Details
CVE-2025-69221	LibreChat is a ChatGPT clone with additional features. Version 0.8.1-rc2 does not enforce proper access control when querying agent permissions. An authenticated attacker can read the permissions of arbitrary agents, even if they have no permissions for this agent. LibreChat allows the configuration of agents that have a predefined set of instructions and context. Private agents are not visible to other users. However, if an attacker knows the agent ID, they can read the permissions of the agent including the permissions individually assigned to other users. This issue is fixed in version 0.8.2-rc2.	4.3	More Details
CVE-2025-14943	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 8.7.2. This is due to a misconfigured authorization check on the 'getShipItemFullText' function which only verifies that a user has the 'read' capability (Subscriber-level) and a valid nonce, but fails to verify whether the user has permission to access the specific post being requested. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract data from password-protected, private, or draft posts.	4.3	More Details
CVE-2026-20936	Out-of-bounds read in Windows NDIS allows an authorized attacker to disclose information with a physical attack.	4.3	More Details
CVE-2026-22605	OpenProject is an open-source, web-based project management software. OpenProject versions prior to version 16.6.3, allowed users with the View Meetings permission on any project, to access meeting details of meetings that belonged to projects, the user does not have access to. This issue has been patched in version 16.6.3.	4.3	More Details
CVE-2025-69333	Missing Authorization vulnerability in Crocoblock JetEngine allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JetEngine: from n/a through 3.8.1.1.	4.3	More Details
CVE-2026-22489	Authorization Bypass Through User-Controlled Key vulnerability in Wptexture Image Slider Slideshow allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Slider Slideshow: from n/a through 1.8.	4.3	More Details
CVE-2025-13990	The Mamurjor Employee Info plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing nonce validation on multiple administrative functions. This makes it possible for unauthenticated attackers to create, update, or delete employee records, departments, designations, salary grades, education records, and salary payments 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-2025-13520	The MTCaptcha WordPress Plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.2. This is due to missing or incorrect nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update the plugin settings, including sensitive values like the private 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-2026-22492	Missing Authorization vulnerability in Nawawi Jamili Docket Cache allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Docket Cache: from n/a through 24.07.04.	4.3	More Details
CVE-2026-21695	Titra is open source project time tracking software. In versions 0.99.49 and below, an API has a Mass Assignment vulnerability which allows authenticated users to inject arbitrary fields into time entries, bypassing business logic controls via the customfields parameter. The affected endpoint uses the JavaScript spread operator (...customfields) to merge user-controlled input directly into the database document. While customfields is validated as an Object type, there is no validation of which keys are permitted inside that object. This allows attackers to overwrite protected fields such as userId, hours, and state. The issue is fixed in version 0.99.50.	4.3	More Details
CVE-2026-22487	Missing Authorization vulnerability in baqend Speed Kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Speed Kit: from n/a through 2.0.2.	4.3	More Details
	The ACF to REST API plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.3.4. This is due to insufficient capability checks in the update_item_permissions_check()		

CVE-2025-12030	method, which only verifies that the current user has the edit_posts capability without checking object-specific permissions (e.g., edit_post($id), edit_user($id), manage_options). This makes it possible for authenticated attackers, with Contributor-level access and above, to modify ACF fields on posts they do not own, any user account, comments, taxonomy terms, and even the global options page via the /wp-json/acf/v3/{type}/{id} endpoints, granted they can authenticate to the site.	4.3	More Details
CVE-2026-0684	The CP Image Store with Slideshow plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.1.9 due to a logic error in the 'cpis_admin_init' function's permission check. This makes it possible for authenticated attackers, with Contributor-level access and above, to import arbitrary products via XML, if the XML file has already been uploaded to the server.	4.3	More Details
CVE-2025-12640	The Folders – Unlimited Folders to Organize Media Library Folder, Pages, Posts, File Manager plugin for WordPress is vulnerable to Unauthorized Arbitrary Media Replacement in all versions up to, and including, 3.1.5. This is due to missing object-level authorization checks in the handle_folders_file_upload() function. This makes it possible for authenticated attackers, with Author-level access and above, to replace arbitrary media files from the WordPress Media Library.	4.3	More Details
CVE-2026-0497	SAP Product Designer Web UI of Business Server Pages allows authenticated non-administrative users to access non-sensitive information. This results in a low impact on confidentiality, with no impact on integrity or availability of the application.	4.3	More Details
CVE-2026-0494	Under certain conditions SAP Fiori App Intercompany Balance Reconciliation application allows an attacker to access information which would otherwise be restricted. This has low impact on confidentiality of the application, integrity and availability are not impacted.	4.3	More Details
CVE-2026-0493	Due to a Cross-Site Request Forgery (CSRF) vulnerability in SAP Fiori App Intercompany Balance Reconciliation an attacker could execute state?changing actions using an inappropriate request type, this deviation from expected request semantics may allow an attacker to trigger unintended actions on behalf of an authenticated user causing low impact on integrity of the system. This has no impact on confidentiality and availability.	4.3	More Details
CVE-2025-13749	The Clearfy Cache – WordPress optimization plugin, Minify HTML, CSS & JS, Defer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.4.0. This is due to missing nonce validation on the "wbcr_upm_change_flag" function. This makes it possible for unauthenticated attackers to disable plugin/theme update notifications 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-2025-66315	There is a configuration defect vulnerability in the version server of ZTE MF258K Pro products. Due to improper directory permission settings, an attacker can execute write permissions in a specific directory.	4.3	More Details
CVE-2025-13393	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.3.1. This is due to insufficient validation of user-supplied URLs before passing them to the getimagesize() function in the Elementor widget integration. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services via the fifu_input_url parameter in the FIFU Elementor widget granted they have permissions to use Elementor.	4.3	More Details
CVE-2025-13657	The HelpDesk contact form plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.5. This is due to missing or incorrect nonce validation on the handle_query_args() function. This makes it possible for unauthenticated attackers to update the plugin's license ID and contact form ID settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13521	The WP Status Notifier 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 settings update functionality. This makes it possible for unauthenticated attackers to update the plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-13527	The xShare plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing nonce validation on the 'xshare_plugin_reset()' function. This makes it possible for unauthenticated attackers to reset the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-0504	Due to insufficient input handling, the SAP Identity Management REST interface allows an authenticated administrator to submit specially crafted malicious REST requests that are processed by JNDI operations without adequate input neutralization. This may lead to limited disclosure or modification of data, resulting in low impact on confidentiality and integrity, with no impact on application availability.	3.8	More Details
CVE-	A Server-Side Request Forgery (SSRF) vulnerability [CWE-918] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.4, FortiSandbox 4.4 all versions, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may		More

2025-67685	allow an authenticated attacker to proxy internal requests limited to plaintext endpoints only via crafted HTTP requests.	3.8	Details
CVE-2025-11235	Unverified Password Change vulnerability in Progress MOVEit Transfer on Windows (REST API modules).This issue affects MOVEit Transfer: from 2023.1.0 before 2023.1.3, from 2023.0.0 before 2023.0.8, from 2022.1.0 before 2022.1.11, from 2022.0.0 before 2022.0.10.	3.7	More Details
CVE-2026-22611	AWS SDK for .NET works with Amazon Web Services to help build scalable solutions with Amazon S3, Amazon DynamoDB, Amazon Glacier, and more. From versions 4.0.0 to before 4.0.3.3, Customer applications could be configured to improperly route AWS API calls to non-existent or non-AWS hosts. This notification is related to the use of specific values for the region input field when calling AWS services. An actor with access to the environment in which the SDK is used could set the region input field to an invalid value. This issue has been patched in version 4.0.3.3.	3.7	More Details
CVE-2026-22602	OpenProject is an open-source, web-based project management software. Prior to version 16.6.2, a low-privileged logged-in user can view the full names of other users. Since user IDs are assigned sequentially and predictably (e.g., 1 to 1000), an attacker can extract a complete list of all users' full names by iterating through these URLs. The same behavior can also be reproduced via the OpenProject API, allowing automated retrieval of full names through the API as well. This issue has been patched in version 16.6.2. Those who are unable to upgrade may apply the patch manually.	3.5	More Details
CVE-2025-62487	### Details On October 1, 2025, Palantir discovered that images uploaded through the Dossier front-end app were not being marked correctly with the proper security levels. The regression was traced back to a change in May 2025, which was meant to allow file uploads to be shared among different artifacts (e.g. other dossiers and presentations). On deployments configured with CBAC, the front-end would present a security picker dialog to set the security level on the uploads, thereby mitigating the issue. On deployments without a CBAC configuration, no security picker dialog appears, leading to a security level of CUSTOM with no markings or datasets selected. The resulting markings and groups for the file uploads thus will be only those added by the "Default authorization rules" defined in the Auth Chooser configuration. On most environments, it is expected that the "Default authorization rules" only add the Everyone group.	3.5	More Details
CVE-2026-0824	A security flaw has been discovered in questdb ui up to 1.11.9. Impacted is an unknown function of the component Web Console. The manipulation results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 1.1.10 is recommended to address this issue. The patch is identified as b42fd9f18476d844ae181a10a249e003dafb823d. You should upgrade the affected component. The vendor confirmed early that the fix "is going to be released as a part of QuestDB 9.3.0" as well.	3.5	More Details
CVE-2025-3950	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.3 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1 that could have allowed a user to leak certain information by referencing specially crafted images that bypass asset proxy protection.	3.5	More Details
CVE-2025-15504	A security flaw has been discovered in lief-project LIEF up to 0.17.1. Affected by this issue is the function Parser::parse_binary of the file src/ELF/Parser.tcc of the component ELF Binary Parser. The manipulation results in null pointer dereference. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.17.2 can resolve this issue. The patch is identified as 81bd5d7ea0c390563f1c4c017c9019d154802978. It is recommended to upgrade the affected component.	3.3	More Details
CVE-2025-15506	A vulnerability was found in AcademySoftwareFoundation OpenColorIO up to 2.5.0. This issue affects the function ConvertToRegularExpression of the file src/OpenColorIO/FileRules.cpp. Performing a manipulation results in out-of-bounds read. The attack needs to be approached locally. The exploit has been made public and could be used. The patch is named ebdbb75123c9d5f4643e041314e2bc988a13f20d. To fix this issue, it is recommended to deploy a patch. The fix was added to the 2.5.1 milestone.	3.3	More Details
CVE-2026-0747	Exposure of sensitive information in the TeamViewer entry dashboard component in Devolutions Remote Desktop Manager 2025.3.24.0 through 2025.3.28.0 on Windows allows an external observer to view a password on screen via a defective masking feature, for example during physical observation or screen sharing.	3.3	More Details
CVE-2025-53470	Out-of-bounds Read vulnerability in Apache NimBLE HCI H4 driver. Specially crafted HCI event could lead to invalid memory read in H4 driver. This issue affects Apache NimBLE: through 1.8. This issue requires a broken or bogus Bluetooth controller and thus severity is considered low. Users are recommended to upgrade to version 1.9, which fixes the issue.	3.1	More Details
CVE-2025-15224	When doing SSH-based transfers using either SCP or SFTP, and asked to do public key authentication, curl would wrongly still ask and authenticate using a locally running SSH agent.	3.1	More Details
CVE-2026-	The User Management Engine (UME) in NetWeaver Application Server for Java (NW AS Java) utilizes an obsolete cryptographic algorithm for encrypting User Mapping data. This weakness could allow an attacker with high-privileged access to exploit the vulnerability under specific conditions potentially leading to partial	3.0	More

0510	disclosure of sensitive information.This has low impact on confidentiality with no impact on integrity and availability of the application.		Details
CVE-2025-31963	Improper authentication and missing CSRF protection in the local setup interface component in HCL BigFix IVR version 4.2 allows a local attacker to perform unauthorized configuration changes via unauthenticated administrative configuration requests.	2.9	More Details
CVE-2025-46676	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS 2023 release versions 7.10.1.0 through 7.10.1.70, contain an Exposure of Sensitive Information to an Unauthorized Actor vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2.7	More Details
CVE-2025-12958	The Rankology SEO and Analytics Tool plugin for WordPress is vulnerable to unauthorized modification of data due to an incorrect capability check on the 'rankology_code_block' page in all versions up to, and including, 2.0. This makes it possible for authenticated attackers, with Editor-level access and above, to add header and footer code blocks.	2.7	More Details
CVE-2026-22250	wlc is a Weblate command-line client using Weblate's REST API. Prior to 1.17.0, the SSL verification would be skipped for some crafted URLs. This vulnerability is fixed in 1.17.0.	2.5	More Details
CVE-2026-22800	PILOS (Platform for Interactive Live-Online Seminars) is a frontend for BigBlueButton. Prior to 4.10.0, Cross-Site Request Forgery (CSRF) vulnerability exists in an administrative API endpoint responsible for terminating all active video conferences on a single server. The affected endpoint performs a destructive action but is exposed via an HTTP GET request. Although proper authorization checks are enforced and the endpoint cannot be triggered cross-site, the use of GET allows the action to be implicitly invoked through same-site content (e.g. embedded resources rendered within the application). As a result, an authenticated administrator who views crafted content within the application may unknowingly trigger the endpoint, causing all active video conferences on the server to be terminated without explicit intent or confirmation. This vulnerability is fixed in 4.10.0.	2.4	More Details
CVE-2026-0730	A flaw has been found in PHPGurukul Staff Leave Management System 1.0. The affected element is the function ADD_STAFF/UPDATE_STAFF of the file /staffleave/slms/slms/adminviews.py of the component SVG File Handler. Executing a manipulation of the argument profile_pic can lead to cross site scripting. The attack can be executed remotely. The exploit has been published and may be used.	2.4	More Details
CVE-2026-0642	A vulnerability was detected in projectworlds House Rental and Property Listing 1.0. This issue affects some unknown processing of the file /app/complaint.php. The manipulation of the argument Name results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2025-15505	A vulnerability was found in Luxul XWR-600 up to 4.0.1. The affected element is an unknown function of the component Web Administration Interface. The manipulation of the argument Guest Network/Wireless Profile SSID results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond with a technical statement.	2.4	More Details
CVE-2025-46643	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS 2023 release versions 7.10.1.0 through 7.10.1.70, contain a Heap-based Buffer Overflow vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service.	2.3	More Details
CVE-2025-31964	Improper service binding configuration in internal service components in HCL BigFix IVR version 4.2 allows a privileged attacker to impact service availability via exposure of administrative services bound to external network interfaces instead of the local authentication interface.	2.2	More Details
CVE-2025-31962	Insufficient session expiration in the Web UI authentication component in HCL BigFix IVR version 4.2 allows an authenticated attacker to gain prolonged unauthorized access to protected API endpoints due to excessive expiration periods.	2.0	More Details
CVE-2025-69273	Improper Authentication vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Authentication Bypass.This issue affects DX NetOps Spectrum: 24.3.10 and earlier.	N/A	More Details
CVE-2025-15479	Stored cross-site scripting (XSS, CWE-79) in the survey content and administration functionality in Data Illusion Zumbrunn NGSurvey Enterprise Edition 3.6.4 on all supported platforms (on Windows and Linux servers) allows authenticated remote users with survey creation or edit privileges to execute arbitrary JavaScript in other users' browsers, steal session information and perform unauthorized actions on their behalf via crafted survey content that is rendered without proper output encoding.	N/A	More Details
CVE-	The massive sending of ARP requests causes a denial of service on one board of the charger that allows		

2026-22540	control of the EV interfaces. Since the board must be operating correctly for the charger to also function correctly.	N/A	More Details
CVE-2026-22535	An attacker with the ability to interact through the network and with access credentials, could, thanks to the unsecured (unencrypted) MQTT communications protocol, write on the server topics of the board that controls the MQTT communications	N/A	More Details
CVE-2025-6225	Kieback&Peter Neutrino-GLT product is used for building management. It's web component "SM70 PHWEB" is vulnerable to shell command injection via login form. The injected commands would execute with low privileges. The vulnerability has been fixed in version 9.40.02	N/A	More Details
CVE-2026-22162	Rejected reason: Not used	N/A	More Details
CVE-2026-22607	Fickling is a Python pickling decompiler and static analyzer. Fickling versions up to and including 0.1.6 do not treat Python's cProfile module as unsafe. Because of this, a malicious pickle that uses cProfile.run() is classified as SUSPICIOUS instead of OVERTLY_MALICIOUS. If a user relies on Fickling's output to decide whether a pickle is safe to deserialize, this misclassification can lead them to execute attacker-controlled code on their system. This affects any workflow or product that uses Fickling as a security gate for pickle deserialization. This issue has been patched in version 0.1.7.	N/A	More Details
CVE-2026-22603	OpenProject is an open-source, web-based project management software. Prior to version 16.6.2, OpenProject’s unauthenticated password-change endpoint (/account/change_password) was not protected by the same brute-force safeguards that apply to the normal login form. In affected versions, an attacker who can guess or enumerate user IDs can send unlimited password-change requests for a given account without triggering lockout or other rate-limiting controls. This allows automated password-guessing (e.g., with wordlists of common passwords) against valid accounts. Successful guessing results in full account compromise for the targeted user and, depending on that user’s role, can lead to further privilege escalation inside the application. This issue has been patched in version 16.6.2. Those who are unable to upgrade may apply the patch manually.	N/A	More Details
CVE-2025-15474	AuntyFey Smart Combination Lock firmware versions as of 2025-12-24 contain a vulnerability that allows an unauthenticated attacker within Bluetooth Low Energy (BLE) range to cause a denial of service by repeatedly initiating BLE connections. Sustained connection attempts interrupt keypad authentication input and repeatedly force the device into lockout states, preventing legitimate users from unlocking the device.	N/A	More Details
CVE-2026-22604	OpenProject is an open-source, web-based project management software. For OpenProject versions from 11.2.1 to before 16.6.2, when sending a POST request to the /account/change_password endpoint with an arbitrary User ID as the password_change_user_id parameter, the resulting error page would show the username for the requested user. Since this endpoint is intended to be called without being authenticated, this allows to enumerate the user names of all accounts registered in an OpenProject instance. This issue has been patched in version 16.6.2.	N/A	More Details
CVE-2025-69271	Insufficiently Protected Credentials vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Sniffing Attacks.This issue affects DX NetOps Spectrum: 24.3.13 and earlier.	N/A	More Details
CVE-2025-69272	Cleartext Transmission of Sensitive Information vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Sniffing Attacks.This issue affects DX NetOps Spectrum: 21.2.1 and earlier.	N/A	More Details
CVE-2026-22606	Fickling is a Python pickling decompiler and static analyzer. Fickling versions up to and including 0.1.6 do not treat Python’s runpy module as unsafe. Because of this, a malicious pickle that uses runpy.run_path() or runpy.run_module() is classified as SUSPICIOUS instead of OVERTLY_MALICIOUS. If a user relies on Fickling’s output to decide whether a pickle is safe to deserialize, this misclassification can lead them to execute attacker-controlled code on their system. This affects any workflow or product that uses Fickling as a security gate for pickle deserialization. This issue has been patched in version 0.1.7.	N/A	More Details
CVE-2026-22158	Rejected reason: Not used	N/A	More Details
CVE-2026-22608	Fickling is a Python pickling decompiler and static analyzer. Prior to version 0.1.7, both ctypes and pydoc modules aren't explicitly blocked. Even other existing pickle scanning tools (like picklescan) do not block pydoc.locate. Chaining these two together can achieve RCE while the scanner still reports the file as LIKELY_SAFE. This issue has been patched in version 0.1.7.	N/A	More Details
CVE-2026-22159	Rejected reason: Not used	N/A	More Details
CVE-			

2026-22157	Rejected reason: Not used	N/A	More Details
CVE-2026-22156	Rejected reason: Not used	N/A	More Details
CVE-2026-20893	Origin validation error issue exists in Fujitsu Security Solution AuthConductor Client Basic V2 2.0.25.0 and earlier. If this vulnerability is exploited, an attacker who can log in to the Windows system where the affected product is installed may execute arbitrary code with SYSTEM privilege and/or modify the registry value.	N/A	More Details
CVE-2026-69267	Improper Limitation of a Pathname to a Restricted Directory (Path Traversal) vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Path Traversal.This issue affects DX NetOps Spectrum: 24.3.8 and earlier.	N/A	More Details
CVE-2026-0650	OpenFlagr versions prior to and including 1.1.18 contain an authentication bypass vulnerability in the HTTP middleware. Due to improper handling of path normalization in the whitelist logic, crafted requests can bypass authentication and access protected API endpoints without valid credentials. Unauthorized access may allow modification of feature flags and export of sensitive data.	N/A	More Details
CVE-2025-69268	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Reflected XSS.This issue affects DX NetOps Spectrum: 24.3.8 and earlier.	N/A	More Details
CVE-2025-69269	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows OS Command Injection.This issue affects DX NetOps Spectrum: 23.3.6 and earlier.	N/A	More Details
CVE-2026-22698	RustCrypto: Elliptic Curves is general purpose Elliptic Curve Cryptography (ECC) support, including types and traits for representing various elliptic curve forms, scalars, points, and public/secret keys composed thereof. In versions 0.14.0-pre.0 and 0.14.0-rc.0, a critical vulnerability exists in the SM2 Public Key Encryption (PKE) implementation where the ephemeral nonce k is generated with severely reduced entropy. A unit mismatch error causes the nonce generation function to request only 32 bits of randomness instead of the expected 256 bits. This reduces the security of the encryption from a 128-bit level to a trivial 16-bit level, allowing a practical attack to recover the nonce k and decrypt any ciphertext given only the public key and ciphertext. This issue has been patched via commit e4f7778.	N/A	More Details
CVE-2025-69270	Information Exposure Through Query Strings in GET Request vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Session Hijacking.This issue affects DX NetOps Spectrum: 24.3.8 and earlier.	N/A	More Details
CVE-2025-14017	When doing multi-threaded LDAPS transfers (LDAP over TLS) with libcurl, changing TLS options in one thread would inadvertently change them globally and therefore possibly also affect other concurrently setup transfers. Disabling certificate verification for a specific transfer could unintentionally disable the feature for other threads as well.	N/A	More Details
CVE-2025-9611	Microsoft Playwright MCP Server versions prior to 0.0.40 fails to validate the Origin header on incoming connections. This allows an attacker to perform a DNS rebinding attack via a victim’s web browser and send unauthorized requests to a locally running MCP server, resulting in unintended invocation of MCP tool endpoints.	N/A	More Details
CVE-2026-22609	Fickling is a Python pickling decompiler and static analyzer. Prior to version 0.1.7, the unsafe_imports() method in Fickling's static analyzer fails to flag several high-risk Python modules that can be used for arbitrary code execution. Malicious pickles importing these modules will not be detected as unsafe, allowing attackers to bypass Fickling's primary static safety checks. This issue has been patched in version 0.1.7.	N/A	More Details
CVE-2026-22542	An attacker with access to the system's internal network can cause a denial of service on the system by making two concurrent connections through the Telnet service.	N/A	More Details
CVE-2026-22160	Rejected reason: Not used	N/A	More Details
CVE-2026-22541	The massive sending of ICMP requests causes a denial of service on one of the boards from the EVCharger that allows control the EV interfaces. Since the board must be operating correctly for the charger to also function correctly.	N/A	More Details
CVE-2026-22691	pypdf is a free and open-source pure-python PDF library. Prior to version 6.6.0, pypdf has possible long runtimes for malformed startxref. An attacker who uses this vulnerability can craft a PDF which leads to possibly long runtimes for invalid startxref entries. When rebuilding the cross-reference table, PDF files with lots of whitespace characters become problematic. Only the non-strict reading mode is affected. Only the	N/A	More Details

	non-strict reading mode is affected. This issue has been patched in version 6.6.0.		
CVE-2026-22601	OpenProject is an open-source, web-based project management software. For OpenProject version 16.6.1 and below, a registered administrator can execute arbitrary command by configuring sendmail binary path and sending a test email. This issue has been patched in version 16.6.2.	N/A	More Details
CVE-2026-22690	pypdf is a free and open-source pure-python PDF library. Prior to version 6.6.0, pypdf has possible long runtimes for missing /Root object with large /Size values. An attacker who uses this vulnerability can craft a PDF which leads to possibly long runtimes for actually invalid files. This can be achieved by omitting the /Root entry in the trailer, while using a rather large /Size value. Only the non-strict reading mode is affected. This issue has been patched in version 6.6.0.	N/A	More Details
CVE-2026-22610	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0, a cross-site scripting (XSS) vulnerability has been identified in the Angular Template Compiler. The vulnerability exists because Angular's internal sanitization schema fails to recognize the href and xlink:href attributes of SVG <script> elements as a Resource URL context. This issue has been patched in versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0.	N/A	More Details
CVE-2026-22597	Ghost is a Node.js content management system. In versions 5.38.0 through 5.130.5 and 6.0.0 through 6.10.3, a vulnerability in Ghost's media inliner mechanism allows staff users in possession of a valid authentication token for the Ghost Admin API to exfiltrate data from internal systems via SSRF. This issue has been patched in versions 5.130.6 and 6.11.0.	N/A	More Details
CVE-2026-22161	Rejected reason: Not used	N/A	More Details
CVE-2026-22612	Fickling is a Python pickling decompiler and static analyzer. Prior to version 0.1.7, Fickling is vulnerable to detection bypass due to "builtins" blindness. This issue has been patched in version 0.1.7.	N/A	More Details
CVE-2026-0675	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-68703	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, the salt is derived from sha256Sum(passphrase). Two encryption operations with the same password will have the same derived key. This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2026-22027	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, the convert_hexstring_to_byte_array() function in the MariaDB SA interface writes decoded bytes into a caller-provided buffer without any capacity check. When importing SA fields from the database (e.g., IV, ARSN, ABM), a malformed or oversized hex string in the database can overflow the destination buffer, corrupting adjacent heap memory. This issue has been patched in version 1.4.3.	N/A	More Details
CVE-2026-22042	RustFS is a distributed object storage system built in Rust. Prior to version 1.0.0-alpha.79, he `ImportIam` admin API validates permissions using `ExportIAMAction` instead of `ImportIAMAction`, allowing a principal with export-only IAM permissions to perform import operations. Since importing IAM data performs privileged write actions (creating/updating users, groups, policies, and service accounts), this can lead to unauthorized IAM modification and privilege escalation. Version 1.0.0-alpha.79 fixes the issue.	N/A	More Details
CVE-2026-20971	Use After Free in PROCA driver prior to SMR Jan-2026 Release 1 allows local attackers to potentially execute arbitrary code.	N/A	More Details
CVE-2026-20972	Improper Export of Android Application Components in UwbTest prior to SMR Jan-2026 Release 1 allows local attackers to enable UWB.	N/A	More Details
CVE-2026-20974	Improper input validation in data related to network restrictions prior to SMR Jan-2026 Release 1 allows physical attackers to bypass Carrier Relock.	N/A	More Details
CVE-2026-20975	Improper handling of insufficient permission in Samsung Cloud prior to version 5.6.11 allows local attackers to access specific files in arbitrary path.	N/A	More Details
CVE-2026-20976	Improper input validation in Galaxy Store prior to version 4.6.02 allows local attacker to execute arbitrary script.	N/A	More Details

CVE-2026-22241	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, an arbitrary file upload vulnerability in the theme import functionality enables an attacker with administrative privileges to upload arbitrary files on the server's file system. The main cause of the issue is that no validation or sanitization of the file's present inside the zip archive. This leads to remote code execution on the web server. Version 4.2 patches the issue.	N/A	More Details
CVE-2026-22043	RustFS is a distributed object storage system built in Rust. In versions 1.0.0-alpha.13 through 1.0.0-alpha.78, a flawed `deny_only` short-circuit in RustFS IAM allows a restricted service account or STS credential to self-issue an unrestricted service account, inheriting the parent’s full privileges. This enables privilege escalation and bypass of session/inline policy restrictions. Version 1.0.0-alpha.79 fixes the issue.	N/A	More Details
CVE-2026-21409	Improper authorization vulnerability exists in RICOH Streamline NX 3.5.1 to 24R3. If a man-in-the-middle attack is conducted on the communication between the affected product and its user, and some crafted request is processed by the product, the user's registration information and/or OIDC (OpenID Connect) tokens may be retrieved.	N/A	More Details
CVE-2026-20969	Improper input validation in SecSettings prior to SMR Jan-2026 Release 1 allows local attacker to access file with system privilege. User interaction is required for triggering this vulnerability.	N/A	More Details
CVE-2026-22034	Snuffleupagus is a module that raises the cost of attacks against website by killing bug classes and providing a virtual patching system. On deployments of Snuffleupagus prior to version 0.13.0 with the non-default upload validation feature enabled and configured to use one of the upstream validation scripts based on Vulcan Logic Disassembler (VLD) while the VLD extension is not available to the CLI SAPI, all files from multipart POST requests are evaluated as PHP code. The issue was fixed in version 0.13.0.	N/A	More Details
CVE-2025-67603	A Improper Authorization vulnerability in Foomuuri llows arbitrary users to influence the firewall configuration.This issue affects Foomuuri: from ? before 0.31.	N/A	More Details
CVE-2025-66003	An External Control of File Name or Path vulnerability in smb4k allowsl ocal users to perform a local root exploit via smb4k mounthelper if they can access and control the contents of a Samba shareThis issue affects smb4k: from ? before 4.0.5.	N/A	More Details
CVE-2026-23478	Cal.com is open-source scheduling software. From 3.1.6 to before 6.0.7, there is a vulnerability in a custom NextAuth JWT callback that allows attackers to gain full authenticated access to any user's account by supplying a target email address via session.update(). This vulnerability is fixed in 6.0.7.	N/A	More Details
CVE-2026-22871	GuardDog is a CLI tool to identify malicious PyPI packages. Prior to 2.7.1, there is a path traversal vulnerability exists in GuardDog's safe_extract() function that allows malicious PyPI packages to write arbitrary files outside the intended extraction directory, leading to Arbitrary File Overwrite and Remote Code Execution on systems running GuardDog. This vulnerability is fixed in 2.7.1.	N/A	More Details
CVE-2026-22870	GuardDog is a CLI tool to identify malicious PyPI packages. Prior to 2.7.1, GuardDog's safe_extract() function does not validate decompressed file sizes when extracting ZIP archives (wheels, eggs), allowing attackers to cause denial of service through zip bombs. A malicious package can consume gigabytes of disk space from a few megabytes of compressed data. This vulnerability is fixed in 2.7.1.	N/A	More Details
CVE-2026-22869	Eigent is a multi-agent Workforce. A critical security vulnerability in the CI workflow (.github/workflows/ci.yml) allows arbitrary code execution from fork pull requests with repository write permissions. The vulnerable workflow uses pull_request_target trigger combined with checkout of untrusted PR code. An attacker can exploit this to steal credentials, post comments, push code, or create releases.	N/A	More Details
CVE-2026-20970	Improper access control in SLocation prior to SMR Jan-2026 Release 1 allows local attackers to execute the privileged APIs.	N/A	More Details
CVE-2026-20968	Use after free in DualDAR prior to SMR Jan-2026 Release 1 allows local privileged attackers to execute arbitrary code.	N/A	More Details
CVE-2026-22026	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, the libcurl write_callback function in the KMC crypto service client allows unbounded memory growth by reallocating response buffers without any size limit or overflow check. A malicious KMC server can return arbitrarily large HTTP responses, forcing the client to allocate excessive memory until the process is terminated by the OS. This issue has been patched in version 1.4.3.	N/A	More Details
CVE-2026-22713	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - GrowthExperiments Extension allows Cross-Site Scripting (XSS).This issue affects Mediawiki - GrowthExperiments Extension: 1.45, 1.44, 1.43, 1.39.	N/A	More Details

CVE-2026-21896	Kirby is an open-source content management system. From versions 5.0.0 to 5.2.1, Kirby is missing permission checks in the content changes API. This vulnerability affects all Kirby sites where user permissions are configured to prevent specific role(s) from performing write actions, specifically by disabling the update permission with the intent to prevent modifications to site content. This vulnerability does not affect those who have not altered the deviated from default user permissions. This issue has been patched in version 5.2.2.	N/A	More Details
CVE-2026-21860	Werkzeug is a comprehensive WSGI web application library. Prior to version 3.1.5, Werkzeug's safe_join function allows path segments with Windows device names that have file extensions or trailing spaces. On Windows, there are special device names such as CON, AUX, etc that are implicitly present and readable in every directory. Windows still accepts them with any file extension, such as CON.txt, or trailing spaces such as CON. This issue has been patched in version 3.1.5.	N/A	More Details
CVE-2026-22245	Mastodon is a free, open-source social network server based on ActivityPub. By nature, Mastodon performs a lot of outbound requests to user-provided domains. Mastodon, however, has some protection mechanism to disallow requests to local IP addresses (unless specified in `ALLOWED_PRIVATE_ADDRESSES`) to avoid the "confused deputy" problem. The list of disallowed IP address ranges was lacking some IP address ranges that can be used to reach local IP addresses. An attacker can use an IP address in the affected ranges to make Mastodon perform HTTP requests against loopback or local network hosts, potentially allowing access to otherwise private resources and services. This is fixed in Mastodon v4.5.4, v4.4.11, v4.3.17 and v4.2.29.	N/A	More Details
CVE-2026-22244	OpenMetadata is a unified metadata platform. Versions prior to 1.11.4 are vulnerable to remote code execution via Server-Side Template Injection (SSTI) in FreeMarker email templates. An attacker must have administrative privileges to exploit the vulnerability. Version 1.11.4 contains a patch.	N/A	More Details
CVE-2025-68151	CoreDNS is a DNS server that chains plugins. Prior to version 1.14.0, multiple CoreDNS server implementations (gRPC, HTTPS, and HTTP/3) lack critical resource-limiting controls. An unauthenticated remote attacker can exhaust memory and degrade or crash the server by opening many concurrent connections, streams, or sending oversized request bodies. The issue is similar in nature to CVE-2025-47950 (QUIC DoS) but affects additional server types that do not enforce connection limits, stream limits, or message size constraints. Version 1.14.0 contains a patch.	N/A	More Details
CVE-2026-22710	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - Wikibase Extension allows Cross-Site Scripting (XSS).This issue affects Mediawiki - Wikibase Extension: 1.45, 1.44, 1.43, 1.39.	N/A	More Details
CVE-2026-22712	Improper Encoding or Escaping of Output due to magic word replacement in ParserAfterTidy vulnerability in The Wikimedia Foundation Mediawiki - ApprovedRevs Extension allows Input Data Manipulation.This issue affects Mediawiki - ApprovedRevs Extension: 1.45, 1.44, 1.43, 1.39.	N/A	More Details
CVE-2026-22714	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - Monaco Skin allows Cross-Site Scripting (XSS).This issue affects Mediawiki - Monaco Skin: 1.45, 1.44, 1.43, 1.39.	N/A	More Details
CVE-2025-67858	A Improper Neutralization of Argument Delimiters vulnerability in Foomuuri can lead to integrity loss of the firewall configuration or further unspecified impact by manipulating the JSON configuration passed to `nft`. This issue affects Foomuuri: from ? before 0.31.	N/A	More Details
CVE-2026-22630	Rejected reason: Not used	N/A	More Details
CVE-2026-22631	Rejected reason: Not used	N/A	More Details
CVE-2026-22632	Rejected reason: Not used	N/A	More Details
CVE-2026-22633	Rejected reason: Not used	N/A	More Details
CVE-2026-22634	Rejected reason: Not used	N/A	More Details
CVE-2026-22635	Rejected reason: Not used	N/A	More Details
CVE-			More

2026-22636	Rejected reason: Not used	N/A	Details
CVE-2026-22868	go-ethereum (geth) is a golang execution layer implementation of the Ethereum protocol. A vulnerable node can be forced to shutdown/crash using a specially crafted message. This vulnerability is fixed in 1.16.8.	N/A	More Details
CVE-2026-22862	go-ethereum (geth) is a golang execution layer implementation of the Ethereum protocol. A vulnerable node can be forced to shutdown/crash using a specially crafted message. This vulnerability is fixed in 1.16.8.	N/A	More Details
CVE-2026-22079	This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the plaintext transmission of login credentials during the initial login or post-factory reset setup through the web-based administrative interface. An attacker on the same network could exploit this vulnerability by intercepting network traffic and capturing the credentials transmitted in plaintext. Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and gain unauthorized access to the targeted device.	N/A	More Details
CVE-2026-22197	GestSup versions up to and including 3.2.56 contain multiple SQL injection vulnerabilities in the asset list functionality. Multiple request parameters used to filter, search, or sort assets are incorporated into SQL queries without sufficient neutralization, allowing an authenticated attacker to manipulate database queries. Successful exploitation can result in unauthorized access to or modification of database contents depending on database privileges.	N/A	More Details
CVE-2026-22537	The lack of hardening of the system allows the user used to manage and maintain the charger to consult different files containing clear-text credentials or valuable information for an attacker.	N/A	More Details
CVE-2025-68702	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, Jervis uses padLeft(32, '0') when it should use padLeft(64, '0') because SHA-256 produces 32 bytes which equates to 64 hex characters. This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2025-68701	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, Jervis uses deterministic AES IV derivation from a passphrase. This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2025-68698	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, Jervis uses PKCS1Encoding which is vulnerable to Bleichenbacher padding oracle attacks. Modern systems should use OAEP (Optimal Asymmetric Encryption Padding). This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2026-22194	GestSup versions up to and including 3.2.56 contain a cross-site request forgery (CSRF) vulnerability where the application does not verify the authenticity of client requests. An attacker can induce a logged-in user to submit crafted requests that perform actions with the victim's privileges. This can be exploited to create privileged accounts by targeting the administrative user creation endpoint.	N/A	More Details
CVE-2026-22195	GestSup versions up to and including 3.2.56 contain a SQL injection vulnerability in the search bar functionality. User-controlled search input is incorporated into SQL queries without sufficient neutralization, allowing an authenticated attacker to manipulate database queries. Successful exploitation can result in unauthorized access to or modification of database contents depending on database privileges.	N/A	More Details
CVE-2026-22196	GestSup versions up to and including 3.2.56 contain a SQL injection vulnerability in ticket creation functionality. User-controlled input provided during ticket creation is incorporated into SQL queries without sufficient neutralization, allowing an authenticated attacker to manipulate database queries. Successful exploitation can result in unauthorized access to or modification of database contents depending on database privileges.	N/A	More Details
CVE-2026-22198	GestSup versions up to and including 3.2.56 contain a pre-authentication stored cross-site scripting (XSS) vulnerability in the API error logging functionality. By sending an API request with a crafted X-API-KEY header value (for example, to /api/v1/ticket.php), an unauthenticated attacker can cause attacker-controlled HTML/JavaScript to be written to log entries. When an administrator later views the affected logs in the web interface, the injected content is rendered without proper output encoding, resulting in arbitrary script execution in the administrator’s browser session.	N/A	More Details
CVE-2026-22080	This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the transmission of credentials encoded using reversible Base64 encoding through the web-based administrative interface. An attacker on the same network could exploit this vulnerability by intercepting network traffic and capturing the Base64-encoded credentials. Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and gain unauthorized access to the targeted device.	N/A	More Details
CVE-2025-8307	Asseco InfoMedica is a comprehensive solution used to manage both administrative and medical tasks in the healthcare sector. Passwords of all users are stored in a database in an encoded format. An attacker in possession of these encoded passwords is able to decode them by using an algorithm embedded in the	N/A	More Details

	client-side part of the software. This vulnerability has been fixed in versions 4.50.1 and 5.38.0		
CVE-2025-14631	A NULL Pointer Dereference vulnerability in TP-Link Archer BE400 V1(802.11 modules) allows an adjacent attacker to cause a denial-of-service (DoS) by triggering a device reboot. This issue affects Archer BE400: xi 1.1.0 Build 20250710 rel.14914.	N/A	More Details
CVE-2025-8306	Asseco InfoMedica is a comprehensive solution used to manage both administrative and medical tasks in the healthcare sector. A low privileged user is able to obtain encoded passwords of all other accounts (including main administrator) due to lack of granularity in access control. Chained exploitation of this vulnerability and CVE-2025-8307 allows an attacker to escalate privileges. This vulnerability has been fixed in versions 4.50.1 and 5.38.0	N/A	More Details
CVE-2026-21900	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, an out-of-bounds heap read vulnerability in cryptography_encrypt() occurs when parsing JSON metadata from KMC server responses. The flawed strtok iteration pattern uses ptr + strlen(ptr) + 1 which reads one byte past allocated buffer boundaries when processing short or malformed metadata strings. This issue has been patched in version 1.4.3.	N/A	More Details
CVE-2026-22023	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, there is an out-of-bounds heap read vulnerability in cryptography_aead_encrypt(). This issue has been patched in version 1.4.3.	N/A	More Details
CVE-2026-22024	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, the cryptography_encrypt() function allocates multiple buffers for HTTP requests and JSON parsing that are never freed on any code path. Each call leaks approximately 400 bytes of memory. Sustained traffic can gradually exhaust available memory. This issue has been patched in version 1.4.3.	N/A	More Details
CVE-2026-22025	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.3, when the KMC server returns a non-200 HTTP status code, cryptography_encrypt() and cryptography_decrypt() return immediately without freeing previously allocated buffers. Each failed request leaks approximately 467 bytes. Repeated failures (from a malicious server or network issues) can gradually exhaust memory. This issue has been patched in version 1.4.3.	N/A	More Details
CVE-2025-68704	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, Jervis uses java.util.Random() which is not cryptographically secure for timing attack mitigation. This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2025-68925	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, the code doesn't validate that the JWT header specifies "alg":"RS256". This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2025-68931	Jervis is a library for Job DSL plugin scripts and shared Jenkins pipeline libraries. Prior to 2.2, AES/CBC/PKCS5Padding lacks authentication, making it vulnerable to padding oracle attacks and ciphertext manipulation. This vulnerability is fixed in 2.2.	N/A	More Details
CVE-2025-69426	The Ruckus vRIoT IoT Controller firmware versions prior to 3.0.0.0 (GA) contain hardcoded credentials for an operating system user account within an initialization script. The SSH service is network-accessible without IP-based restrictions. Although the configuration disables SCP and pseudo-TTY allocation, an attacker can authenticate using the hardcoded credentials and establish SSH local port forwarding to access the Docker socket. By mounting the host filesystem via Docker, an attacker can escape the container and execute arbitrary OS commands as root on the underlying vRIoT controller, resulting in complete system compromise.	N/A	More Details
CVE-2025-66049	Vivotek IP7137 camera with firmware version 0200a is vulnerable to an information disclosure issue where live camera footage can be accessed through the RTSP protocol on port 8554 without requiring authentication. This allows unauthorized users with network access to view the camera's feed, potentially compromising user privacy and security. The vendor has not replied to the CNA. Possibly all firmware versions are affected. Since the product has met End-Of-Life phase, a fix is not expected to be released.	N/A	More Details
CVE-2025-66050	Vivotek IP7137 camera with firmware version 0200a by default dos not require to provide any password when logging in as an administrator. While it is possible to set up such a password, a user is not informed about such a need. The vendor has not replied to the CNA. Possibly all firmware versions are affected. Since the product has met End-Of-Life phase, a fix is not expected to be released.	N/A	More Details
CVE-2025-66051	Vivotek IP7137 camera with firmware version 0200a is vulnerable to path traversal. It is possible for an authenticated attacker to access resources beyond webroot directory using a direct HTTP request. Due to CVE-2025-66050, a password for administration panel is not set by default. The vendor has not replied to the CNA. Possibly all firmware versions are affected. Since the product has met End-Of-Life phase, a fix is not	N/A	More Details

	expected to be released.		
CVE-2025-66052	Vivotek IP7137 camera with firmware version 0200a is vulnerable to command injection. Parameter "system_ntpIt" used by "/cgi-bin/admin/setparam.cgi" endpoint is not sanitized properly, allowing a user with administrative privileges to perform an attack. Due to CVE-2025-66050, administrative access is not protected by default, The vendor has not replied to the CNA Possibly all firmware versions are affected. Since the product has met End-Of-Life phase, a fix is not expected to be released.	N/A	More Details
CVE-2025-7072	The firmware in KAON CG3000TC and CG3000T routers contains hard-coded credentials in clear text (shared across all routers of this model) that an unauthenticated remote attacker could use to execute commands with root privileges. This vulnerability has been fixed in firmware version: 1.00.67 for CG3000TC and 1.00.27 for CG3000T.	N/A	More Details
CVE-2026-22081	This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the missing HTTPOnly flag for session cookies associated with the web-based administrative interface. A remote at-tacker could exploit this vulnerability by capturing session cookies transmitted over an insecure HTTP connection. Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and gain unau-thorized access to the targeted device.	N/A	More Details
CVE-2026-22082	This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the use of login credentials as the session ID through its web-based administrative interface. A remote attacker could exploit this vulnerability by intercepting network traffic and capturing the session ID during insecure transmission. Successful exploitation of this vulnerability could allow the attacker to hijack an authenticated session and compromise sensitive configuration information on the targeted device.	N/A	More Details
CVE-2025-66002	An Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability allows local users ton perform arbitrary unmounts via smb4k mount helper	N/A	More Details
CVE-2025-15056	A lack of data validation vulnerability in the HTML export feature in Quill in allows Cross-Site Scripting (XSS). This issue affects Quill: 2.0.3.	N/A	More Details
CVE-2025-4596	Asseco ADMX system is used for processing medical records. It allows logged in users to access medical files belonging to other users through manipulation of GET arguments containing document IDs. This issue has been fixed in 6.09.01.62 version of ADMX.	N/A	More Details
CVE-2020-36875	AccessAlly WordPress plugin versions prior to 3.3.2 contain an unauthenticated arbitrary PHP code execution vulnerability in the Login Widget. The plugin processes the login_error parameter as PHP code, allowing an attacker to supply and execute arbitrary PHP in the context of the WordPress web server process, resulting in remote code execution.	N/A	More Details
CVE-2026-22814	@adonisjs/lucid is an SQL ORM for AdonisJS built on top of Knex. Prior to 21.8.2 and 22.0.0-next.6, there is a Mass Assignment vulnerability in AdonisJS Lucid which may allow a remote attacker who can influence data that is passed into Lucid model assignments to overwrite the internal ORM state. This may lead to logic bypasses and unauthorized record modification within a table or model. This affects @adonisjs/lucid through version 21.8.1 and 22.x pre-release versions prior to 22.0.0-next.6. This has been patched in @adonisjs/lucid versions 21.8.2 and 22.0.0-next.6.	N/A	More Details
CVE-2025-15035	Improper Input Validation vulnerability in TP-Link Archer AXE75 v1.6 (vpn modules) allows an authenticated adjacent attacker to delete arbitrary server file, leading to possible loss of critical system files and service interruption or degraded functionality.This issue affects Archer AXE75 v1.6: ≤ build 20250107.	N/A	More Details
CVE-2026-21895	The `rsa` crate is an RSA implementation written in rust. Prior to version 0.9.10, when creating a RSA private key from its components, the construction panics instead of returning an error when one of the primes is `1`. Version 0.9.10 fixes the issue.	N/A	More Details
CVE-2025-69425	The Ruckus vRIoT IoT Controller firmware versions prior to 3.0.0.0 (GA) expose a command execution service on TCP port 2004 running with root privileges. Authentication to this service relies on a hardcoded Time-based One-Time Password (TOTP) secret and an embedded static token. An attacker who extracts these credentials from the appliance or a compromised device can generate valid authentication tokens and execute arbitrary OS commands with root privileges, resulting in complete system compromise.	N/A	More Details
CVE-2026-22536	The absence of permissions control for the user XXX allows the current configuration in the sudoers file to escalate privileges without any restrictions	N/A	More Details
CVE-2026-22835	Rejected reason: Not used	N/A	More Details
CVE-2026-	The credentials required to access the device's web server are sent in base64 within the HTTP headers. Since base64 is not considered a strong cipher, an attacker could intercept the web request handling the login and	N/A	More

22543	obtain the credentials		Details
CVE-2025-68800	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_mr: Fix use-after-free when updating multicast route stats Cited commit added a dedicated mutex (instead of RTNL) to protect the multicast route list, so that it will not change while the driver periodically traverses it in order to update the kernel about multicast route stats that were queried from the device. One instance of list entry deletion (during route replace) was missed and it can result in a use-after-free [1]. Fix by acquiring the mutex before deleting the entry from the list and releasing it afterwards. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_mr_stats_update+0x4a5/0x540 drivers/net/ethernet/mellanox/mlxsw/spectrum_mr.c:1006 [mlxsw_spectrum] Read of size 8 at addr ffff8881523c2fa8 by task kworker/2:5/22043 CPU: 2 UID: 0 PID: 22043 Comm: kworker/2:5 Not tainted 6.18.0-rc1-custom-g1a3d6d7cd014 #1 PREEMPT(full) Hardware name: Mellanox Technologies Ltd. MSN2010/SA002610, BIOS 5.6.5 08/24/2017 Workqueue: mlxsw_core mlxsw_sp_mr_stats_update [mlxsw_spectrum] Call Trace: <TASK> dump_stack_lvl+0xba/0x110 print_report+0x174/0x4f5 kasan_report+0xdf/0x110 mlxsw_sp_mr_stats_update+0x4a5/0x540 drivers/net/ethernet/mellanox/mlxsw/spectrum_mr.c:1006 [mlxsw_spectrum] process_one_work+0x9cc/0x18e0 worker_thread+0x5df/0xe40 kthread+0x3b8/0x730 ret_from_fork+0x3e9/0x560 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 29933: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 mlxsw_sp_mr_route_add+0xd8/0x4770 [mlxsw_spectrum] mlxsw_sp_router_fibmr_event_work+0x371/0xad0 drivers/net/ethernet/mellanox/mlxsw/spectrum_router.c:7965 [mlxsw_spectrum] process_one_work+0x9cc/0x18e0 worker_thread+0x5df/0xe40 kthread+0x3b8/0x730 ret_from_fork+0x3e9/0x560 ret_from_fork_asm+0x1a/0x30 Freed by task 29933: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_save_free_info+0x3b/0x70 __kasan_slab_free+0x43/0x70 kfree+0x14e/0x700 mlxsw_sp_mr_route_add+0x2dea/0x4770 drivers/net/ethernet/mellanox/mlxsw/spectrum_mr.c:444 [mlxsw_spectrum] mlxsw_sp_router_fibmr_event_work+0x371/0xad0 drivers/net/ethernet/mellanox/mlxsw/spectrum_router.c:7965 [mlxsw_spectrum] process_one_work+0x9cc/0x18e0 worker_thread+0x5df/0xe40 kthread+0x3b8/0x730 ret_from_fork+0x3e9/0x560 ret_from_fork_asm+0x1a/0x30	N/A	More Details
CVE-2025-68809	In the Linux kernel, the following vulnerability has been resolved: ksmbd: vfs: fix race on m_flags in vfs_cache ksmbd maintains delete-on-close and pending-delete state in ksmbd_inode->m_flags. In vfs_cache.c this field is accessed under inconsistent locking: some paths read and modify m_flags under ci->m_lock while others do so without taking the lock at all. Examples: - ksmbd_query_inode_status() and __ksmbd_inode_close() use ci->m_lock when checking or updating m_flags. - ksmbd_inode_pending_delete(), ksmbd_set_inode_pending_delete(), ksmbd_clear_inode_pending_delete() and ksmbd_fd_set_delete_on_close() used to read and modify m_flags without ci->m_lock. This creates a potential data race on m_flags when multiple threads open, close and delete the same file concurrently. In the worst case delete-on-close and pending-delete bits can be lost or observed in an inconsistent state, leading to confusing delete semantics (files that stay on disk after delete-on-close, or files that disappear while still in use). Fix it by: - Making ksmbd_query_inode_status() look at m_flags under ci->m_lock after dropping inode_hash_lock. - Adding ci->m_lock protection to all helpers that read or modify m_flags (ksmbd_inode_pending_delete(), ksmbd_set_inode_pending_delete(), ksmbd_clear_inode_pending_delete(), ksmbd_fd_set_delete_on_close()). - Keeping the existing ci->m_lock protection in __ksmbd_inode_close(), and moving the actual unlink/xattr removal outside the lock. This unifies the locking around m_flags and removes the data race while preserving the existing delete-on-close behaviour.	N/A	More Details
CVE-2025-68808	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: initialize local pointers upon transfer of memory ownership vidtv_channel_si_init() creates a temporary list (program, service, event) and ownership of the memory itself is transferred to the PAT/SDT/EIT tables through vidtv_psi_pat_program_assign(), vidtv_psi_sdt_service_assign(), vidtv_psi_eit_event_assign(). The problem here is that the local pointer where the memory ownership transfer was completed is not initialized to NULL. This causes the vidtv_psi_pmt_create_sec_for_each_pat_entry() function to fail, and in the flow that jumps to free_eit, the memory that was freed by vidtv_psi_*_table_destroy() can be accessed again by vidtv_psi_*_event_destroy() due to the uninitialized local pointer, so it is freed once again. Therefore, to prevent use-after-free and double-free vulnerability, local pointers must be initialized to NULL when transferring memory ownership.	N/A	More Details
CVE-2025-68807	In the Linux kernel, the following vulnerability has been resolved: block: fix race between wbt_enable_default and IO submission When wbt_enable_default() is moved out of queue freezing in elevator_change(), it can cause the wbt inflight counter to become negative (-1), leading to hung tasks in the writeback path. Tasks get stuck in wbt_wait() because the counter is in an inconsistent state. The issue occurs because wbt_enable_default() could race with IO submission, allowing the counter to be decremented before proper initialization. This manifests as: rq_wait[0]: inflight: -1 has_waiters: True rwb_enabled() checks the state, which can be updated exactly between wbt_wait() (rq_qos_throttle()) and wbt_track()(rq_qos_track()), then the inflight counter will become negative. And results in hung task warnings like: task:kworker/u24:39 state:D stack:0 pid:14767 Call Trace: rq_qos_wait+0xb4/0x150 wbt_wait+0xa9/0x100 __rq_qos_throttle+0x24/0x40 blk_mq_submit_bio+0x672/0x7b0 ... Fix this by: 1. Splitting wbt_enable_default() into: - __wbt_enable_default(): Returns true if wbt_init() should be called - wbt_enable_default(): Wrapper for existing callers (no init) - wbt_init_enable_default(): New function that checks and inits WBT 2. Using	N/A	More Details

	wbt_init_enable_default() in blk_register_queue() to ensure proper initialization during queue registration 3. Move wbt_init() out of wbt_enable_default() which is only for enabling disabled wbt from bfq and iocost, and wbt_init() isn't needed. Then the original lock warning can be avoided. 4. Removing the ELEVATOR_FLAG_ENABLE_WBT_ON_EXIT flag and its handling code since it's no longer needed This ensures WBT is properly initialized before any IO can be submitted, preventing the counter from going negative.		
CVE-2025-68806	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix buffer validation by including null terminator size in EA length The smb2_set_ea function, which handles Extended Attributes (EA), was performing buffer validation checks that incorrectly omitted the size of the null terminating character (+1 byte) for EA Name. This patch fixes the issue by explicitly adding '+ 1' to EaNameLength where the null terminator is expected to be present in the buffer, ensuring the validation accurately reflects the total required buffer size.	N/A	More Details
CVE-2025-68805	In the Linux kernel, the following vulnerability has been resolved: fuse: fix io-uring list corruption for terminated non-committed requests When a request is terminated before it has been committed, the request is not removed from the queue's list. This leaves a dangling list entry that leads to list corruption and use-after-free issues. Remove the request from the queue's list for terminated non-committed requests.	N/A	More Details
CVE-2025-68804	In the Linux kernel, the following vulnerability has been resolved: platform/chrome: cros_ec_ishtp: Fix UAF after unbinding driver After unbinding the driver, another kthread `cros_ec_console_log_work` is still accessing the device, resulting an UAF and crash. The driver doesn't unregister the EC device in .remove() which should shutdown sub-devices synchronously. Fix it.	N/A	More Details
CVE-2025-68803	In the Linux kernel, the following vulnerability has been resolved: NFSD: NFSv4 file creation neglects setting ACL An NFSv4 client that sets an ACL with a named principal during file creation retrieves the ACL afterwards, and finds that it is only a default ACL (based on the mode bits) and not the ACL that was requested during file creation. This violates RFC 8881 section 6.4.1.3: "the ACL attribute is set as given". The issue occurs in nfsd_create_setattr(), which calls nfsd_attrs_valid() to determine whether to call nfsd_setattr(). However, nfsd_attrs_valid() checks only for iattr changes and security labels, but not POSIX ACLs. When only an ACL is present, the function returns false, nfsd_setattr() is skipped, and the POSIX ACL is never applied to the inode. Subsequently, when the client retrieves the ACL, the server finds no POSIX ACL on the inode and returns one generated from the file's mode bits rather than returning the originally-specified ACL.	N/A	More Details
CVE-2025-68802	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Limit num_syncs to prevent oversized allocations The exec and vm_bind ioctl allow userspace to specify an arbitrary num_syncs value. Without bounds checking, a very large num_syncs can force an excessively large allocation, leading to kernel warnings from the page allocator as below. Introduce DRM_XE_MAX_SYNCS (set to 1024) and reject any request exceeding this limit. " ------------[cut here]------------ WARNING: CPU: 0 PID: 1217 at mm/page_alloc.c:5124 __alloc_frozen_pages_noprof+0x2f8/0x2180 mm/page_alloc.c:5124 ... Call Trace: <TASK> alloc_pages_mpol+0xe4/0x330 mm/mempolicy.c:2416 ___kmalloc_large_node+0xd8/0x110 mm/slub.c:4317 __kmalloc_large_node_noprof+0x18/0xe0 mm/slub.c:4348 __do_kmalloc_node mm/slub.c:4364 [inline] __kmalloc_noprof+0x3d4/0x4b0 mm/slub.c:4388 kmalloc_noprof include/linux/slab.h:909 [inline] kmalloc_array_noprof include/linux/slab.h:948 [inline] xe_exec_ioctl+0xa47/0x1e70 drivers/gpu/drm/xe/xe_exec.c:158 drm_ioctl_kernel+0x1f1/0x3e0 drivers/gpu/drm/drm_ioctl.c:797 drm_ioctl+0x5e7/0xc50 drivers/gpu/drm/drm_ioctl.c:894 xe_drm_ioctl+0x10b/0x170 drivers/gpu/drm/xe/xe_device.c:224 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:598 [inline] __se_sys_ioctl fs/ioctl.c:584 [inline] __x64_sys_ioctl+0x18b/0x210 fs/ioctl.c:584 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xbb/0x380 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... " v2: Add "Reported-by" and Cc stable kernels. v3: Change XE_MAX_SYNCS from 64 to 1024. (Matt & Ashutosh) v4: s/XE_MAX_SYNCS/DRM_XE_MAX_SYNCS/ (Matt) v5: Do the check at the top of the exec func. (Matt) (cherry picked from commit b07bac9bd708ec468cd1b8a5fe70ae2ac9b0a11c)	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_router: Fix neighbour use-after-free We sometimes observe use-after-free when dereferencing a neighbour [1]. The problem seems to be that the driver stores a pointer to the neighbour, but without holding a reference on it. A reference is only taken when the neighbour is used by a nexthop. Fix by simplifying the reference counting scheme. Always take a reference when storing a neighbour pointer in a neighbour entry. Avoid taking a referencing when the neighbour is used by a nexthop as the neighbour entry associated with the nexthop already holds a reference. Tested by running the test that uncovered the problem over 300 times. Without this patch the problem was reproduced after a handful of iterations. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_neigh_entry_update+0x2d4/0x310 Read of size 8 at addr ffff88817f8e3420 by task ip/3929 CPU: 3 UID: 0 PID: 3929 Comm: ip Not tainted 6.18.0-rc4-virtme-g36b21a067510 #3 PREEMPT(full) Hardware name: Nvidia SN5600/VMOD0013, BIOS 5.13 05/31/2023 Call Trace: <TASK> dump_stack_lvl+0x6f/0xa0 print_address_description.constprop.0+0x6e/0x300 print_report+0xfc/0x1fb kasan_report+0xe4/0x110 mlxsw_sp_neigh_entry_update+0x2d4/0x310 mlxsw_sp_router_rif_gone_sync+0x35f/0x510 mlxsw_sp_rif_destroy+0x1ea/0x730 mlxsw_sp_inetaddr_port_vlan_event+0xa1/0x1b0 __mlxsw_sp_inetaddr_lag_event+0xcc/0x130 __mlxsw_sp_inetaddr_event+0xf5/0x3c0 mlxsw_sp_router_netdevice_event+0x1015/0x1580 notifier_call_chain+0xcc/0x150 call_netdevice_notifiers_info+0x7e/0x100 __netdev_upper_dev_unlink+0x10b/0x210 netdev_upper_dev_unlink+0x79/0xa0 vrf_del_slave+0x18/0x50 do_set_master+0x146/0x7d0		

CVE-2025-68801	do_setlink.isra.0+0x9a0/0x2880 rtnl_newlink+0x637/0xb20 rtnetlink_rcv_msg+0x6fe/0xb90 netlink_rcv_skb+0x123/0x380 netlink_unicast+0x4a3/0x770 netlink_sendmsg+0x75b/0xc90 __sock_sendmsg+0xbe/0x160 ____sys_sendmsg+0x5b2/0x7d0 ___sys_sendmsg+0xfd/0x180 __sys_sendmsg+0x124/0x1c0 do_syscall_64+0xbb/0xfd0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [...] Allocated by task 109: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x7b/0x90 __kmalloc_noprof+0x2c1/0x790 neigh_alloc+0x6af/0x8f0 ___neigh_create+0x63/0xe90 mlxsw_sp_nexthop_neigh_init+0x430/0x7e0 mlxsw_sp_nexthop_type_init+0x212/0x960 mlxsw_sp_nexthop6_group_info_init.constprop.0+0x81f/0x1280 mlxsw_sp_nexthop6_group_get+0x392/0x6a0 mlxsw_sp_fib6_entry_create+0x46a/0xfd0 mlxsw_sp_router_fib6_replace+0x1ed/0x5f0 mlxsw_sp_router_fib6_event_work+0x10a/0x2a0 process_one_work+0xd57/0x1390 worker_thread+0x4d6/0xd40 kthread+0x355/0x5b0 ret_from_fork+0x1d4/0x270 ret_from_fork_asm+0x11/0x20 Freed by task 154: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_save_free_info+0x3b/0x60 __kasan_slab_free+0x43/0x70 kmem_cache_free_bulk.part.0+0x1eb/0x5e0 kvfree_rcu_bulk+0x1f2/0x260 kfree_rcu_work+0x130/0x1b0 process_one_work+0xd57/0x1390 worker_thread+0x4d6/0xd40 kthread+0x355/0x5b0 ret_from_fork+0x1d4/0x270 ret_from_fork_asm+0x11/0x20 Last potentially related work creation: kasan_save_stack+0x30/0x50 kasan_record_aux_stack+0x8c/0xa0 kvfree_call_rcu+0x93/0x5b0 mlxsw_sp_router_neigh_event_work+0x67d/0x860 process_one_work+0xd57/0x1390 worker_thread+0x4d6/0xd40 kthread+0x355/0x5b0 ret_from_fork+0x1d4/0x270 ret_from_fork_asm+0x11/0x20	N/A	More Details
CVE-2025-68799	In the Linux kernel, the following vulnerability has been resolved: caif: fix integer underflow in cffrml_receive() The cffrml_receive() function extracts a length field from the packet header and, when FCS is disabled, subtracts 2 from this length without validating that len >= 2. If an attacker sends a malicious packet with a length field of 0 or 1 to an interface with FCS disabled, the subtraction causes an integer underflow. This can lead to memory exhaustion and kernel instability, potential information disclosure if padding contains uninitialized kernel memory. Fix this by validating that len >= 2 before performing the subtraction.	N/A	More Details
CVE-2025-68811	In the Linux kernel, the following vulnerability has been resolved: svcrdma: use rc_pageoff for memcpy byte offset svc_rdma_copy_inline_range added rc_curpage (page index) to the page base instead of the byte offset rc_pageoff. Use rc_pageoff so copies land within the current page. Found by ZeroPath (https://zeropath.com)	N/A	More Details
CVE-2025-68798	In the Linux kernel, the following vulnerability has been resolved: perf/x86/amd: Check event before enable to avoid GPF On AMD machines cpuc->events[idx] can become NULL in a subtle race condition with NMI->throttle->x86_pmu_stop(). Check event for NULL in amd_pmu_enable_all() before enable to avoid a GPF. This appears to be an AMD only issue. Syzkaller reported a GPF in amd_pmu_enable_all. INFO: NMI handler (perf_event_nmi_handler) took too long to run: 13.143 msecs Oops: general protection fault, probably for non-canonical address 0xdfffffc0000000034: 0000 PREEMPT SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x00000000000001a0-0x00000000000001a7] CPU: 0 UID: 0 PID: 328415 Comm: repro_36674776 Not tainted 6.12.0-rc1-syzk RIP: 0010:x86_pmu_enable_event (arch/x86/events/perf_event.h:1195 arch/x86/events/core.c:1430) RSP: 0018:ffff888118009d60 EFLAGS: 00010012 RAX: dfffffc0000000000 RBX: 0000000000000000 RCX: 0000000000000000 RDX: 0000000000000034 RSI: 0000000000000000 RDI: 00000000000001a0 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000002 R13: ffff88811802a440 R14: ffff88811802a240 R15: ffff8881132d8601 FS: 00007f097dfaa700(0000) GS:ffff888118000000(0000) GS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000200001c0 CR3: 0000000103d56000 CR4: 00000000000006f0 Call Trace: <IRQ> amd_pmu_enable_all (arch/x86/events/amd/core.c:760 (discriminator 2)) x86_pmu_enable (arch/x86/events/core.c:1360) event_sched_out (kernel/events/core.c:1191 kernel/events/core.c:1186 kernel/events/core.c:2346) __perf_remove_from_context (kernel/events/core.c:2435) event_function (kernel/events/core.c:259) remote_function (kernel/events/core.c:92 (discriminator 1) kernel/events/core.c:72 (discriminator 1)) __flush_smp_call_function_queue (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:207 ./include/trace/events/csd.h:64 kernel/smp.c:135 kernel/smp.c:540) __sysvec_call_function_single (./arch/x86/include/asm/jump_label.h:27 ./include/linux/jump_label.h:207 ./arch/x86/include/asm/trace/irq_vectors.h:99 arch/x86/kernel/smp.c:272) sysvec_call_function_single (arch/x86/kernel/smp.c:266 (discriminator 47) arch/x86/kernel/smp.c:266 (discriminator 47)) </IRQ>	N/A	More Details
CVE-2025-68797	In the Linux kernel, the following vulnerability has been resolved: char: applicom: fix NULL pointer dereference in ac_ioctl Discovered by Atuin - Automated Vulnerability Discovery Engine. In ac_ioctl, the validation of IndexCard and the check for a valid RamIO pointer are skipped when cmd is 6. However, the function unconditionally executes readb(apbs[IndexCard].RamIO + VERS) at the end. If cmd is 6, IndexCard may reference a board that does not exist (where RamIO is NULL), leading to a NULL pointer dereference. Fix this by skipping the readb access when cmd is 6, as this command is a global information query and does not target a specific board context.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid updating zero-sized extent in extent cache As syzbot reported: F2FS-fs (loop0): __update_extent_tree_range: extent len is zero, type: 0, extent [0, 0, 0], age [0, 0] ------------[cut here]------------ kernel BUG at fs/f2fs/extent_cache.c:678! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 0 UID: 0 PID: 5336 Comm: syz.0.0 Not tainted syzkaller #0		

CVE-2025-68796	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:__update_extent_tree_range+0x13bc/0x1500 fs/f2fs/extent_cache.c:678 Call Trace: <TASK> f2fs_update_read_extent_cache_range+0x192/0x3e0 fs/f2fs/extent_cache.c:1085 f2fs_do_zero_range fs/f2fs/file.c:1657 [inline] f2fs_zero_range+0x10c1/0x1580 fs/f2fs/file.c:1737 f2fs_fallocate+0x583/0x990 fs/f2fs/file.c:2030 vfs_fallocate+0x669/0x7e0 fs/open.c:342 ioctl_preallocate fs/ioctl.c:289 [inline] file_ioctl+0x611/0x780 fs/ioctl.c:-1 do_vfs_ioctl+0xb33/0x1430 fs/ioctl.c:576 __do_sys_ioctl fs/ioctl.c:595 [inline] __se_sys_ioctl+0x82/0x170 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f07bc58eec9 In error path of f2fs_zero_range(), it may add a zero-sized extent into extent cache, it should be avoided.	N/A	More Details
CVE-2025-68795	In the Linux kernel, the following vulnerability has been resolved: ethtool: Avoid overflowing userspace buffer on stats query The ethtool -S command operates across three ioctl calls: ETHTOOL_GSSET_INFO for the size, ETHTOOL_GSTRINGS for the names, and ETHTOOL_GSTATS for the values. If the number of stats changes between these calls (e.g., due to device reconfiguration), userspace's buffer allocation will be incorrect, potentially leading to buffer overflow. Drivers are generally expected to maintain stable stat counts, but some drivers (e.g., mlx5, bnx2x, bna, ksz884x) use dynamic counters, making this scenario possible. Some drivers try to handle this internally: - bnad_get_ethtool_stats() returns early in case stats.n_stats is not equal to the driver's stats count. - micrel/ksz884x also makes sure not to write anything beyond stats.n_stats and overflow the buffer. However, both use stats.n_stats which is already assigned with the value returned from get_sset_count(), hence won't solve the issue described here. Change ethtool_get_strings(), ethtool_get_stats(), ethtool_get_phy_stats() to not return anything in case of a mismatch between userspace's size and get_sset_size(), to prevent buffer overflow. The returned n_stats value will be equal to zero, to reflect that nothing has been returned. This could result in one of two cases when using upstream ethtool, depending on when the size change is detected: 1. When detected in ethtool_get_strings(): # ethtool -S eth2 no stats available 2. When detected in get stats, all stats will be reported as zero. Both cases are presumably transient, and a subsequent ethtool call should succeed. Other than the overflow avoidance, these two cases are very evident (no output/cleared stats), which is arguably better than presenting incorrect/shifted stats. I also considered returning an error instead of a "silent" response, but that seems more destructive towards userspace apps. Notes: - This patch does not claim to fix the inherent race, it only makes sure that we do not overflow the userspace buffer, and makes for a more predictable behavior. - RTNL lock is held during each ioctl, the race window exists between the separate ioctl calls when the lock is released. - Userspace ethtool always fills stats.n_stats, but it is likely that these stats ioctls are implemented in other userspace applications which might not fill it. The added code checks that it's not zero, to prevent any regressions.	N/A	More Details
CVE-2025-68794	In the Linux kernel, the following vulnerability has been resolved: iomap: adjust read range correctly for non-block-aligned positions iomap_adjust_read_range() assumes that the position and length passed in are block-aligned. This is not always the case however, as shown in the syzbot generated case for erofs. This causes too many bytes to be skipped for uptodate blocks, which results in returning the incorrect position and length to read in. If all the blocks are uptodate, this underflows length and returns a position beyond the folio. Fix the calculation to also take into account the block offset when calculating how many bytes can be skipped for uptodate blocks.	N/A	More Details
CVE-2025-68793	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix a job->pasid access race in gpu recovery Avoid a possible UAF in GPU recovery due to a race between the sched timeout callback and the tdr work queue. The gpu recovery function calls drm_sched_stop() and later drm_sched_start(). drm_sched_start() restarts the tdr queue which will eventually free the job. If the tdr queue frees the job before time out callback completes, the job will be freed and we'll get a UAF when accessing the pasid. Cache it early to avoid the UAF. Example KASAN trace: [493.058141] BUG: KASAN: slab-use-after-free in amdgpu_device_gpu_recover+0x968/0x990 [amdgpu] [493.067530] Read of size 4 at addr ffff88b0ce3f794c by task kworker/u128:1/323 [493.074892] [493.076485] CPU: 9 UID: 0 PID: 323 Comm: kworker/u128:1 Tainted: G E 6.16.0-1289896.2.zuul.bf4f11df81c1410bbe901c4373305a31 #1 PREEMPT(voluntary) [493.076493] Tainted: [E]=UNSIGNED_MODULE [493.076495] Hardware name: TYAN B8021G88V2HR-2T/S8021GM2NR-2T, BIOS V1.03.B10 04/01/2019 [493.076500] Workqueue: amdgpu-reset-dev drm_sched_job_timedout [gpu_sched] [493.076512] Call Trace: [493.076515] <TASK> [493.076518] dump_stack_lvl+0x64/0x80 [493.076529] print_report+0xce/0x630 [493.076536] ? _raw_spin_lock_irqsave+0x86/0xd0 [493.076541] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [493.076545] ? amdgpu_device_gpu_recover+0x968/0x990 [amdgpu] [493.077253] kasan_report+0xb8/0xf0 [493.077258] ? amdgpu_device_gpu_recover+0x968/0x990 [amdgpu] [493.077965] amdgpu_device_gpu_recover+0x968/0x990 [amdgpu] [493.078672] ? __pfx_amdgpu_device_gpu_recover+0x10/0x10 [amdgpu] [493.079378] ? amdgpu_coredump+0x1fd/0x4c0 [amdgpu] [493.080111] amdgpu_job_timedout+0x642/0x1400 [amdgpu] [493.080903] ? pick_task_fair+0x24e/0x330 [493.080910] ? __pfx_amdgpu_job_timedout+0x10/0x10 [amdgpu] [493.081702] ? _raw_spin_lock+0x75/0xc0 [493.081708] ? __pfx__raw_spin_lock+0x10/0x10 [493.081712] drm_sched_job_timedout+0x1b0/0x4b0 [gpu_sched] [493.081721] ? __pfx__raw_spin_lock_irq+0x10/0x10 [493.081725] process_one_work+0x679/0xff0 [493.081732] worker_thread+0x6ce/0xfd0 [493.081736] ? __pfx_worker_thread+0x10/0x10 [493.081739] kthread+0x376/0x730 [493.081744] ? __pfx_kthread+0x10/0x10 [493.081748] ? __pfx__raw_spin_lock_irq+0x10/0x10 [493.081751] ? __pfx_kthread+0x10/0x10 [493.081755] ret_from_fork+0x247/0x330 [493.081761] ? __pfx_kthread+0x10/0x10 [493.081764] ret_from_fork_asm+0x1a/0x30 [493.081771] </TASK> (cherry	N/A	More Details

	picked from commit 20880a3fd5dd7bca1a079534cf6596bda92e107d)		
CVE-2025-68792	In the Linux kernel, the following vulnerability has been resolved: tpm2-sessions: Fix out of range indexing in name_size 'name_size' does not have any range checks, and it just directly indexes with TPM_ALG_ID, which could lead into memory corruption at worst. Address the issue by only processing known values and returning -EINVAL for unrecognized values. Make also 'tpm_buf_append_name' and 'tpm_buf_fill_hmac_session' fallible so that errors are detected before causing any spurious TPM traffic. End also the authorization session on failure in both of the functions, as the session state would be then by definition corrupted.	N/A	More Details
CVE-2025-68791	In the Linux kernel, the following vulnerability has been resolved: fuse: missing copy_finish in fuse-over-io-uring argument copies Fix a possible reference count leak of payload pages during fuse argument copies. [Joanne: simplified error cleanup]	N/A	More Details
CVE-2025-68790	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix double unregister of HCA_PORTS component Clear hca_devcom_comp in device's private data after unregistering it in LAG teardown. Otherwise a slightly lagging second pass through mlx5_unload_one() might try to unregister it again and trip over use-after-free. On s390 almost all PCI level recovery events trigger two passes through mxl5_unload_one() - one through the poll_health() method and one through mlx5_pci_err_detected() as callback from generic PCI error recovery. While testing PCI error recovery paths with more kernel debug features enabled, this issue reproducibly led to kernel panics with the following call chain: Unable to handle kernel pointer dereference in virtual kernel address space Failing address: 6b6b6b6b6b6b6000 TEID: 6b6b6b6b6b6b6803 ESOP-2 FSI Fault in home space mode while using kernel ASCE. AS:00000000705c4007 R3:0000000000000024 Oops: 0038 ilc:3 [#1]SMP CPU: 14 UID: 0 PID: 156 Comm: kmcheck Kdump: loaded Not tainted 6.18.0-20251130.rc7.git0.16131a59cab1.300.fc43.s390x+debug #1 PREEMPT Krnl PSW : 0404e00180000000 0000020fc86aa1dc (__lock_acquire+0x5c/0x15f0) R:0 T:1 IO:0 EX:0 Key:0 M:1 W:0 P:0 AS:3 CC:2 PM:0 RI:0 EA:3 Krnl GPRS: 0000000000000000 0000020f00000001 6b6b6b6b6b6b6c33 0000000000000000 0000000000000000 0000000000000000 0000000000000001 0000000000000000 0000000000000000 0000020fca28b820 0000000000000000 0000010a1ced8100 0000010a1ced8100 0000020fc9775068 0000018fce14f8b8 0000018fce14f7f8 Krnl Code: 0000020fc86aa1cc: e3b003400004 lg %r11,832 0000020fc86aa1d2: a7840211 brc 8,0000020fc86aa5f4 *0000020fc86aa1d6: c09000df0b25 larl %r9,0000020fca28b820 >0000020fc86aa1dc: d50790002000 clc 0(8,%r9),0(%r2) 0000020fc86aa1e2: a7840209 brc 8,0000020fc86aa5f4 0000020fc86aa1e6: c0e001100401 larl %r14,0000020fca8aa9e8 0000020fc86aa1ec: c01000e25a00 larl %r1,0000020fca2f55ec 0000020fc86aa1f2: a7eb00e8 aghi %r14,232 Call Trace: __lock_acquire+0x5c/0x15f0 lock_acquire.part.0+0xf8/0x270 lock_acquire+0xb0/0x1b0 down_write+0x5a/0x250 mlx5_detach_device+0x42/0x110 [mlx5_core] mlx5_unload_one_devl_locked+0x50/0xc0 [mlx5_core] mlx5_unload_one+0x42/0x60 [mlx5_core] mlx5_pci_err_detected+0x94/0x150 [mlx5_core] zpci_event_attempt_error_recovery+0xcc/0x388	N/A	More Details
CVE-2025-68810	In the Linux kernel, the following vulnerability has been resolved: KVM: Disallow toggling KVM_MEM_GUEST_MEMFD on an existing memslot Reject attempts to disable KVM_MEM_GUEST_MEMFD on a memslot that was initially created with a guest_memfd binding, as KVM doesn't support toggling KVM_MEM_GUEST_MEMFD on existing memslots. KVM prevents enabling KVM_MEM_GUEST_MEMFD, but doesn't prevent clearing the flag. Failure to reject the new memslot results in a use-after-free due to KVM not unbinding from the guest_memfd instance. Unbinding on a FLAGS_ONLY change is easy enough, and can/will be done as a hardening measure (in anticipation of KVM supporting dirty logging on guest_memfd at some point), but fixing the use-after-free would only address the immediate symptom. == BUG: KASAN: slab-use-after-free in kvm_gmem_release+0x362/0x400 [kvm] Write of size 8 at addr ffff8881111ae908 by task repro/745 CPU: 7 UID: 1000 PID: 745 Comm: repro Not tainted 6.18.0-rc6-115d5de2eef3-next-kasan #3 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 Call Trace: <TASK> dump_stack_lvl+0x51/0x60 print_report+0xcb/0x5c0 kasan_report+0xb4/0xe0 kvm_gmem_release+0x362/0x400 [kvm] __fput+0x2fa/0x9d0 task_work_run+0x12c/0x200 do_exit+0x6ae/0x2100 do_group_exit+0xa8/0x230 __x64_sys_exit_group+0x3a/0x50 x64_sys_call+0x737/0x740 do_syscall_64+0x5b/0x900 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f581f2eac31 </TASK> Allocated by task 745 on cpu 6 at 9.746971s: kasan_save_stack+0x20/0x40 kasan_save_track+0x13/0x50 __kasan_kmalloc+0x77/0x90 kvm_set_memory_region.part.0+0x652/0x1110 [kvm] kvm_vm_ioctl+0x14b0/0x3290 [kvm] __x64_sys_ioctl+0x129/0x1a0 do_syscall_64+0x5b/0x900 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 745 on cpu 6 at 9.747467s: kasan_save_stack+0x20/0x40 kasan_save_track+0x13/0x50 __kasan_save_free_info+0x37/0x50 __kasan_slab_free+0x3b/0x60 kfree+0xf5/0x440 kvm_set_memslot+0x3c2/0x1160 [kvm] kvm_set_memory_region.part.0+0x86a/0x1110 [kvm] kvm_vm_ioctl+0x14b0/0x3290 [kvm] __x64_sys_ioctl+0x129/0x1a0 do_syscall_64+0x5b/0x900 entry_SYSCALL_64_after_hwframe+0x4b/0x53	N/A	More Details
CVE-2025-68812	In the Linux kernel, the following vulnerability has been resolved: media: iris: Add sanity check for stop streaming Add sanity check in iris_vb2_stop_streaming. If inst->state is already IRIS_INST_ERROR, we should skip the stream_off operation because it would still send packets to the firmware. In iris_kill_session, inst->state is set to IRIS_INST_ERROR and session_close is executed, which will kfree(inst_hfi_gen2->packet). If stop_streaming is called afterward, it will cause a crash. [bod: remove qcom from patch title]	N/A	More Details

CVE-2025-71066	In the Linux kernel, the following vulnerability has been resolved: net/sched: ets: Always remove class from active list before deleting in ets_qdisc_change zdi-disclosures@trendmicro.com says: The vulnerability is a race condition between `ets_qdisc_dequeue` and `ets_qdisc_change`. It leads to UAF on `struct Qdisc` object. Attacker requires the capability to create new user and network namespace in order to trigger the bug. See my additional commentary at the end of the analysis. Analysis: static int ets_qdisc_change(struct Qdisc *sch, struct nlattr *opt, struct netlink_ext_ack *extack) { ... // (1) this lock is preventing .change handler (`ets_qdisc_change`) //to race with .dequeue handler (`ets_qdisc_dequeue`) sch_tree_lock(sch); for (i = nbands; i < oldbands; i++) { if (i >= q->nstrict && q->classes[i].qdisc->q.qlen) list_del_init(&q->classes[i].alist); qdisc_purge_queue(q->classes[i].qdisc); } WRITE_ONCE(q->nbands, nbands); for (i = nstrict; i < q->nstrict; i++) { if (q->classes[i].qdisc->q.qlen) { // (2) the class is added to the q->active list_add_tail(&q->classes[i].alist, &q->active); q->classes[i].deficit = quanta[i]; } } WRITE_ONCE(q->nstrict, nstrict); memcpy(q->prio2band, priomap, sizeof(priomap)); for (i = 0; i < q->nbands; i++) WRITE_ONCE(q->classes[i].quantum, quanta[i]); for (i = oldbands; i < q->nbands; i++) { q->classes[i].qdisc = queues[i]; if (q->classes[i].qdisc != &noop_qdisc) qdisc_hash_add(q->classes[i].qdisc, true); } // (3) the qdisc is unlocked, now dequeue can be called in parallel // to the rest of .change handler sch_tree_unlock(sch); ets_offload_change(sch); for (i = q->nbands; i < oldbands; i++) { // (4) we're reducing the refcount for our class's qdisc and // freeing it qdisc_put(q->classes[i].qdisc); // (5) If we call .dequeue between (4) and (5), we will have // a strong UAF and we can control RIP q->classes[i].qdisc = NULL; WRITE_ONCE(q->classes[i].quantum, 0); q->classes[i].deficit = 0; gnet_stats_basic_sync_init(&q->classes[i].bstats); memset(&q->classes[i].qstats, 0, sizeof(q->classes[i].qstats)); } return 0; } Comment: This happens because some of the classes have their qdiscs assigned to NULL, but remain in the active list. This commit fixes this issue by always removing the class from the active list before deleting and freeing its associated qdisc Reproducer Steps (trimmed version of what was sent by zdi-disclosures@trendmicro.com) ``` DEV="${DEV:-lo}" ROOT_HANDLE="${ROOT_HANDLE:-1:}" BAND2_HANDLE="${BAND2_HANDLE:-20:}" # child under 1:2 PING_BYTES="${PING_BYTES:-48}" PING_COUNT="${PING_COUNT:-200000}" PING_DST="${PING_DST:-127.0.0.1}" SLOW_TBF_RATE="${SLOW_TBF_RATE:-8bit}" SLOW_TBF_BURST="${SLOW_TBF_BURST:-100b}" SLOW_TBF_LAT="${SLOW_TBF_LAT:-1s}" cleanup() { tc qdisc del dev "$DEV" root 2>/dev/null } trap cleanup EXIT ip link set "$DEV" up tc qdisc del dev "$DEV" root 2>/dev/null || true tc qdisc add dev "$DEV" root handle "$ROOT_HANDLE" ets bands 2 strict 2 tc qdisc add dev "$DEV" parent 1:2 handle "$BAND2_HANDLE" \ tbf rate "$SLOW_TBF_RATE" burst "$SLOW_TBF_BURST" latency "$SLOW_TBF_LAT" tc filter add dev "$DEV" parent 1: protocol all prio 1 u32 match u32 0 0 flowid 1:2 tc -s qdisc ls dev $DEV ping -I "$DEV" -f -c "$PING_COUNT" -s "$PING_BYTES" -W 0.001 "$PING_DST" \ >/dev/null 2>&1 & tc qdisc change dev "$DEV" root handle "$ROOT_HANDLE" ets bands 2 strict 0 tc qdisc change dev "$DEV" root handle "$ROOT_HANDLE" ets bands 2 strict 2 tc -s qdisc ls dev $DEV tc qdisc del dev "$DEV" parent ---truncated---	N/A	More Details
CVE-2025-69990	phpgurukul News Portal Project V4.1 has an Arbitrary File Deletion Vulnerability in remove_file.php. The parameter file can cause any file to be deleted.	N/A	More Details
CVE-2025-71064	In the Linux kernel, the following vulnerability has been resolved: net: hns3: using the num_tqps in the vf driver to apply for resources Currently, hdev->htqp is allocated using hdev->num_tqps, and kinfo->tqp is allocated using kinfo->num_tqps. However, kinfo->num_tqps is set to min(new_tqps, hdev->num_tqps); Therefore, kinfo->num_tqps may be smaller than hdev->num_tqps, which causes some hdev->htqp[i] to remain uninitialized in hclgevf_knic_setup(). Thus, this patch allocates hdev->htqp and kinfo->tqp using hdev->num_tqps, ensuring that the lengths of hdev->htqp and kinfo->tqp are consistent and that all elements are properly initialized.	N/A	More Details
CVE-2025-71027	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow in the wanMTU2 parameter of the fromAdvSetMacMtuWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-71026	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow in the wanSpeed2 parameter of the fromAdvSetMacMtuWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-71025	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow in the cloneType2 parameter of the fromAdvSetMacMtuWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-71024	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow in the serviceName2 parameter of the fromAdvSetMacMtuWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2026-22213	RIOT OS versions up to and including 2026.01-devel-317 contain a stack-based buffer overflow vulnerability in the tapslip6 utility. The vulnerability is caused by unsafe string concatenation in the devopen() function, which constructs a device path using unbounded user-controlled input. The utility uses strcpy() and strcat() to concatenate the fixed prefix '/dev/' with a user-supplied device name provided via the -s command-line option without bounds checking. This allows an attacker to supply an excessively long device name and overflow a fixed-size stack buffer, leading to process crashes and memory corruption.	N/A	More Details
CVE-	Tenda AX-1806 v1.0.0.1 was discovered to contain a stack overflow in the security_5g parameter of the		

2025-70753	sub_4CA50 function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-69992	phpgurukul News Portal Project V4.1 has File Upload Vulnerability via upload.php, which enables the upload of files of any format to the server without identity authentication.	N/A	More Details
CVE-2025-69991	phpgurukul News Portal Project V4.1 is vulnerable to SQL Injection in check_availablity.php.	N/A	More Details
CVE-2025-68823	In the Linux kernel, the following vulnerability has been resolved: ublk: fix deadlock when reading partition table When one process(such as udev) opens ublk block device (e.g., to read the partition table via bdev_open()), a deadlock[1] can occur: 1. bdev_open() grabs disk->open_mutex 2. The process issues read I/O to ublk backend to read partition table 3. In __ublk_complete_rq(), blk_update_request() or blk_mq_end_request() runs bio->bi_end_io() callbacks 4. If this triggers fput() on file descriptor of ublk block device, the work may be deferred to current task's task work (see fput() implementation) 5. This eventually calls blkdev_release() from the same context 6. blkdev_release() tries to grab disk->open_mutex again 7. Deadlock: same task waiting for a mutex it already holds The fix is to run blk_update_request() and blk_mq_end_request() with bottom halves disabled. This forces blkdev_release() to run in kernel work-queue context instead of current task work context, and allows ublk server to make forward progress, and avoids the deadlock. [axboe: rewrite comment in ublk]	N/A	More Details
CVE-2025-68813	In the Linux kernel, the following vulnerability has been resolved: ipvs: fix ipv4 null-ptr-deref in route error path The IPv4 code path in __ip_vs_get_out_rt() calls dst_link_failure() without ensuring skb->dev is set, leading to a NULL pointer dereference in fib_compute_spec_dst() when ipv4_link_failure() attempts to send ICMP destination unreachable messages. The issue emerged after commit ed0de45a1008 ("ipv4: recompile ip options in ipv4_link_failure") started calling __ip_options_compile() from ipv4_link_failure(). This code path eventually calls fib_compute_spec_dst() which dereferences skb->dev. An attempt was made to fix the NULL skb->dev dereference in commit 0113d9c9d1cc ("ipv4: fix null-deref in ipv4_link_failure"), but it only addressed the immediate dev_net(skb->dev) dereference by using a fallback device. The fix was incomplete because fib_compute_spec_dst() later in the call chain still accesses skb->dev directly, which remains NULL when IPVS calls dst_link_failure(). The crash occurs when: 1. IPVS processes a packet in NAT mode with a misconfigured destination 2. Route lookup fails in __ip_vs_get_out_rt() before establishing a route 3. The error path calls dst_link_failure(skb) with skb->dev == NULL 4. ipv4_link_failure() → ipv4_send_dest_unreach() → __ip_options_compile() → fib_compute_spec_dst() 5. fib_compute_spec_dst() dereferences NULL skb->dev Apply the same fix used for IPv6 in commit 326bf17ea5d4 ("ipvs: fix ipv6 route unreach panic"): set skb->dev from skb_dst(skb)->dev before calling dst_link_failure(). KASAN: null-ptr-deref in range [0x0000000000000328-0x000000000000032f] CPU: 1 PID: 12732 Comm: syz.1.3469 Not tainted 6.6.114 #2 RIP: 0010:__in_dev_get_rcu include/linux/inetdevice.h:233 RIP: 0010:fib_compute_spec_dst+0x17a/0x9f0 net/ipv4/fib_frontend.c:285 Call Trace: <TASK> spec_dst_fill net/ipv4/ip_options.c:232 spec_dst_fill net/ipv4/ip_options.c:229 __ip_options_compile+0x13a1/0x17d0 net/ipv4/ip_options.c:330 ipv4_send_dest_unreach net/ipv4/route.c:1252 ipv4_link_failure+0x702/0xb80 net/ipv4/route.c:1265 dst_link_failure include/net/dst.h:437 __ip_vs_get_out_rt+0x15fd/0x19e0 net/netfilter/ipvs/ip_vs_xmit.c:412 ip_vs_nat_xmit+0x1d8/0xc80 net/netfilter/ipvs/ip_vs_xmit.c:764	N/A	More Details
CVE-2025-68822	In the Linux kernel, the following vulnerability has been resolved: Input: alps - fix use-after-free bugs caused by dev3_register_work The dev3_register_work delayed work item is initialized within alps_reconnect() and scheduled upon receipt of the first bare PS/2 packet from an external PS/2 device connected to the ALPS touchpad. During device detachment, the original implementation calls flush_workqueue() in psmouse_disconnect() to ensure completion of dev3_register_work. However, the flush_workqueue() in psmouse_disconnect() only blocks and waits for work items that were already queued to the workqueue prior to its invocation. Any work items submitted after flush_workqueue() is called are not included in the set of tasks that the flush operation awaits. This means that after flush_workqueue() has finished executing, the dev3_register_work could still be scheduled. Although the psmouse state is set to PSMOUSE_CMD_MODE in psmouse_disconnect(), the scheduling of dev3_register_work remains unaffected. The race condition can occur as follows: CPU 0 (cleanup path) | CPU 1 (delayed work) psmouse_disconnect() | psmouse_set_state() | flush_workqueue() | alps_report_bare_ps2_packet() alps_disconnect() | psmouse_queue_work() kfree(priv); // FREE | alps_register_bare_ps2_mouse() | priv = container_of(work...); // USE | priv->dev3 // USE Add disable_delayed_work_sync() in alps_disconnect() to ensure that dev3_register_work is properly canceled and prevented from executing after the alps_data structure has been deallocated. This bug is identified by static analysis.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: fuse: fix readahead reclaim deadlock Commit e26ee4efbc79 ("fuse: allocate ff->release_args only if release is needed") skips allocating ff->release_args if the server does not implement open. However in doing so, fuse_prepare_release() now skips grabbing the reference on the inode, which makes it possible for an inode to be evicted from the dcache while there are inflight readahead requests. This causes a deadlock if the server triggers reclaim while servicing the readahead request and reclaim attempts to evict the inode of the file being read ahead. Since the folio is locked during readahead, when reclaim evicts the fuse inode and fuse_evict_inode() attempts to		

CVE-2025-68821	remove all folios associated with the inode from the page cache (truncate_inode_pages_range()), reclaim will block forever waiting for the lock since readahead cannot relinquish the lock because it is itself blocked in reclaim: >>> stack_trace(1504735) folio_wait_bit_common (mm/filemap.c:1308:4) folio_lock (./include/linux/pagemap.h:1052:3) truncate_inode_pages_range (mm/truncate.c:336:10) fuse_evict_inode (fs/fuse/inode.c:161:2) evict (fs/inode.c:704:3) dentry_unlink_inode (fs/dcache.c:412:3) __dentry_kill (fs/dcache.c:615:3) shrink_kill (fs/dcache.c:1060:12) shrink_dentry_list (fs/dcache.c:1087:3) prune_dcache_sb (fs/dcache.c:1168:2) super_cache_scan (fs/super.c:221:10) do_shrink_slab (mm/shrinker.c:435:9) shrink_slab (mm/shrinker.c:626:10) shrink_node (mm/vmscan.c:5951:2) shrink_zones (mm/vmscan.c:6195:3) do_try_to_free_pages (mm/vmscan.c:6257:3) do_swap_page (mm/memory.c:4136:11) handle_pte_fault (mm/memory.c:5562:10) handle_mm_fault (mm/memory.c:5870:9) do_user_addr_fault (arch/x86/mm/fault.c:1338:10) handle_page_fault (arch/x86/mm/fault.c:1481:3) exc_page_fault (arch/x86/mm/fault.c:1539:2) asm_exc_page_fault+0x22/0x27 Fix this deadlock by allocating ff->release_args and grabbing the reference on the inode when preparing the file for release even if the server does not implement open. The inode reference will be dropped when the last reference on the fuse file is dropped (see fuse_file_put() -> fuse_release_end()).	N/A	More Details
CVE-2025-68820	In the Linux kernel, the following vulnerability has been resolved: ext4: xattr: fix null pointer deref in ext4_raw_inode() If ext4_get_inode_loc() fails (e.g. if it returns -EFSCORRUPTED), iloc.bh will remain set to NULL. Since ext4_xattr_inode_dec_ref_all() lacks error checking, this will lead to a null pointer dereference in ext4_raw_inode(), called right after ext4_get_inode_loc(). Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-68819	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb: dtv5100: fix out-of-bounds in dtv5100_i2c_msg() rlen value is a user-controlled value, but dtv5100_i2c_msg() does not check the size of the rlen value. Therefore, if it is set to a value larger than sizeof(st->data), an out-of-bounds vuln occurs for st->data. Therefore, we need to add proper range checking to prevent this vuln.	N/A	More Details
CVE-2025-68818	In the Linux kernel, the following vulnerability has been resolved: scsi: Revert "scsi: qla2xxx: Perform lockless command completion in abort path" This reverts commit 0367076b0817d5c75dfb83001ce7ce5c64d803a9. The commit being reverted added code to __qla2x00_abort_all_cmds() to call sp->done() without holding a spinlock. But unlike the older code below it, this new code failed to check sp->cmd_type and just assumed TYPE_SRB, which results in a jump to an invalid pointer in target-mode with TYPE_TGT_CMD: qla2xxx [0000:65:00.0]-d034:8: qla24xx_do_nack_work create sess success 0000000009f7a79b qla2xxx [0000:65:00.0]-5003:8: ISP System Error - mbx1=1ff5h mbx2=10h mbx3=0h mbx4=0h mbx5=191h mbx6=0h mbx7=0h. qla2xxx [0000:65:00.0]-d01e:8: -> fwdump no buffer qla2xxx [0000:65:00.0]-f03a:8: qla_target(0): System error async event 0x8002 occurred qla2xxx [0000:65:00.0]-00af:8: Performing ISP error recovery - ha=0000000058183fda. BUG: kernel NULL pointer dereference, address: 0000000000000000 PF: supervisor instruction fetch in kernel mode PF: error_code(0x0010) - not-present page PGD 0 P4D 0 Oops: 0010 [#1] SMP CPU: 2 PID: 9446 Comm: qla2xxx_8_dpc Tainted: G O 6.1.133 #1 Hardware name: Supermicro Super Server/X11SPL-F, BIOS 4.2 12/15/2023 RIP: 0010:0x0 Code: Unable to access opcode bytes at 0xffffffffffffffd6. RSP: 0018:ffffc90001f93dc8 EFLAGS: 00010206 RAX: 0000000000000282 RBX: 0000000000000355 RCX: ffff88810d16a000 RDX: ffff88810dbadaa8 RSI: 0000000000080000 RDI: ffff888169dc38c0 RBP: ffff888169dc38c0 R08: 0000000000000001 R09: 0000000000000045 R10: ffffffffa034bdf0 R11: 0000000000000000 R12: ffff88810800bb40 R13: 0000000000001aa8 R14: ffff888100136610 R15: ffff8881070f7400 FS: 0000000000000000(0000) GS:ffff88bf80080000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffffffffffffd6 CR3: 000000010c8ff006 CR4: 0000000003706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? __die+0x4d/0x8b ? page_fault_oops+0x91/0x180 ? trace_buffer_unlock_commit_regs+0x38/0x1a0 ? exc_page_fault+0x391/0x5e0 ? asm_exc_page_fault+0x22/0x30 __qla2x00_abort_all_cmds+0xcb/0x3e0 [qla2xxx_scst] qla2x00_abort_all_cmds+0x50/0x70 [qla2xxx_scst] qla2x00_abort_isp_cleanup+0x3b7/0x4b0 [qla2xxx_scst] qla2x00_abort_isp+0xfd/0x860 [qla2xxx_scst] qla2x00_do_dpc+0x581/0xa40 [qla2xxx_scst] kthread+0xa8/0xd0 </TASK> Then commit 4475afa2646d ("scsi: qla2xxx: Complete command early within lock") added the spinlock back, because not having the lock caused a race and a crash. But qla2x00_abort_srb() in the switch below already checks for qla2x00_chip_is_down() and handles it the same way, so the code above the switch is now redundant and still buggy in target-mode. Remove it.	N/A	More Details
CVE-2025-68817	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_tree_connect_put under concurrency Under high concurrency, A tree-connection object (tcon) is freed on a disconnect path while another path still holds a reference and later executes *_put()/write on it.	N/A	More Details
CVE-2025-68816	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fw_tracer, Validate format string parameters Add validation for format string parameters in the firmware tracer to prevent potential security vulnerabilities and crashes from malformed format strings received from firmware. The firmware tracer receives format strings from the device firmware and uses them to format trace messages. Without proper validation, bad firmware could provide format strings with invalid format specifiers (e.g., %s, %p, %n) that could lead to crashes, or other undefined behavior. Add mlx5_tracer_validate_params() to validate that all format specifiers in trace strings are limited to safe integer/hex formats (%x, %d, %i, %u, %llx, %lx, etc.). Reject strings containing other format types that could be used to access arbitrary memory or cause crashes. Invalid format strings are added to the trace output for visibility with "BAD_FORMAT: " prefix.	N/A	More Details

CVE-2025-68815	In the Linux kernel, the following vulnerability has been resolved: net/sched: ets: Remove drr class from the active list if it changes to strict Whenever a user issues an ets qdisc change command, transforming a drr class into a strict one, the ets code isn't checking whether that class was in the active list and removing it. This means that, if a user changes a strict class (which was in the active list) back to a drr one, that class will be added twice to the active list [1]. Doing so with the following commands: tc qdisc add dev lo root handle 1: ets bands 2 strict 1 tc qdisc add dev lo parent 1:2 handle 20: \ tbf rate 8bit burst 100b latency 1s tc filter add dev lo parent 1: basic classid 1:2 ping -c1 -W0.01 -s 56 127.0.0.1 tc qdisc change dev lo root handle 1: ets bands 2 strict 2 tc qdisc change dev lo root handle 1: ets bands 2 strict 1 ping -c1 -W0.01 -s 56 127.0.0.1 Will trigger the following splat with list debug turned on: [59.279014][T365] ------------[cut here]------------ [59.279452][T365] list_add double add: new=ffff88801d60e350, prev=ffff88801d60e350, next=ffff88801d60e2c0. [59.280153][T365] WARNING: CPU: 3 PID: 365 at lib/list_debug.c:35 __list_add_valid_or_report+0x17f/0x220 [59.280860][T365] Modules linked in: [59.281165][T365] CPU: 3 UID: 0 PID: 365 Comm: tc Not tainted 6.18.0-rc7-00105-g7e9f13163c13-dirty #239 PREEMPT(voluntary) [59.281977][T365] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [59.282391][T365] RIP: 0010:__list_add_valid_or_report+0x17f/0x220 [59.282842][T365] Code: 89 c6 e8 d4 b7 0d ff 90 0f 0b 90 90 31 c0 e9 31 ff ff ff 90 48 c7 c7 e0 a0 22 9f 48 89 f2 48 89 c1 4c 89 c6 e8 b2 b7 0d ff 90 <0f> 0b 90 90 31 c0 e9 0f ff ff ff 48 89 f7 48 89 44 24 10 4c 89 44 ... [59.288812][T365] Call Trace: [59.289056][T365] <TASK> [59.289224][T365] ? srso_alias_return_thunk+0x5/0xfbef5 [59.289546][T365] ets_qdisc_change+0xd2b/0x1e80 [59.289891][T365] ? __lock_acquire+0x7e7/0x1be0 [59.290223][T365] ? __pfx_ets_qdisc_change+0x10/0x10 [59.290546][T365] ? srso_alias_return_thunk+0x5/0xfbef5 [59.290898] [T365] ? __mutex_trylock_common+0xda/0x240 [59.291228][T365] ? __pfx___mutex_trylock_common+0x10/0x10 [59.291655][T365] ? srso_alias_return_thunk+0x5/0xfbef5 [59.291993][T365] ? srso_alias_return_thunk+0x5/0xfbef5 [59.292313][T365] ? trace_contention_end+0xc8/0x110 [59.292656][T365] ? srso_alias_return_thunk+0x5/0xfbef5 [59.293022][T365] ? srso_alias_return_thunk+0x5/0xfbef5 [59.293351][T365] tc_modify_qdisc+0x63a/0x1cf0 Fix this by always checking and removing an ets class from the active list when changing it to strict. [1] https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/tree/net/sched/sch_ets.c?id=ce052b9402e461a9aded599f5b47e76bc727f7de#n663	N/A	More Details
CVE-2025-68814	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix filename leak in __io_openat_prep() __io_openat_prep() allocates a struct filename using getname(). However, for the condition of the file being installed in the fixed file table as well as having O_CLOEXEC flag set, the function returns early. At that point, the request doesn't have REQ_F_NEED_CLEANUP flag set. Due to this, the memory for the newly allocated struct filename is not cleaned up, causing a memory leak. Fix this by setting the REQ_F_NEED_CLEANUP for the request just after the successful getname() call, so that when the request is torn down, the filename will be cleaned up, along with other resources needing cleanup.	N/A	More Details
CVE-2025-68789	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ibmpex) fix use-after-free in high/low store The ibmpex_high_low_store() function retrieves driver data using dev_get_drvdata() and uses it without validation. This creates a race condition where the sysfs callback can be invoked after the data structure is freed, leading to use-after-free. Fix by adding a NULL check after dev_get_drvdata(), and reordering operations in the deletion path to prevent TOCTOU.	N/A	More Details
CVE-2025-68788	In the Linux kernel, the following vulnerability has been resolved: fsnotify: do not generate ACCESS/MODIFY events on child for special files inotify/fanotify do not allow users with no read access to a file to subscribe to events (e.g. IN_ACCESS/IN_MODIFY), but they do allow the same user to subscribe for watching events on children when the user has access to the parent directory (e.g. /dev). Users with no read access to a file but with read access to its parent directory can still stat the file and see if it was accessed/modified via atime/mtime change. The same is not true for special files (e.g. /dev/null). Users will not generally observe atime/mtime changes when other users read/write to special files, only when someone sets atime/mtime via utimensat(). Align fsnotify events with this stat behavior and do not generate ACCESS/MODIFY events to parent watchers on read/write of special files. The events are still generated to parent watchers on utimensat(). This closes some side-channels that could be possibly used for information exfiltration [1]. [1] https://snee.la/pdf/pubs/file-notification-attacks.pdf	N/A	More Details
CVE-2025-68787	In the Linux kernel, the following vulnerability has been resolved: netrom: Fix memory leak in nr_sendmsg() syzbot reported a memory leak [1]. When function sock_alloc_send_skb() return NULL in nr_output(), the original skb is not freed, which was allocated in nr_sendmsg(). Fix this by freeing it before return. [1] BUG: memory leak unreferenced object 0xffff888129f35500 (size 240): comm "syz.0.17", pid 6119, jiffies 4294944652 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 10 52 28 81 88 ff ff .....R(.... backtrace (crc 1456a3e4): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4983 [inline] slab_alloc_node mm/slub.c:5288 [inline] kmem_cache_alloc_node_noprof+0x36f/0x5e0 mm/slub.c:5340 __alloc_skb+0x203/0x240 net/core/skbuff.c:660 alloc_skb include/linux/skbuff.h:1383 [inline] alloc_skb_with_frags+0x69/0x3f0 net/core/skbuff.c:6671 sock_alloc_send_pskb+0x379/0x3e0 net/core/sock.c:2965 sock_alloc_send_skb include/net/sock.h:1859 [inline] nr_sendmsg+0x287/0x450 net/netrom/af_netrom.c:1105 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] sock_write_iter+0x293/0x2a0 net/socket.c:1195 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x45d/0x710 fs/read_write.c:686 ksys_write+0x143/0x170 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xa4/0xfa0	N/A	More Details

	arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f		
CVE-2026-22830	Rejected reason: Not used	N/A	More Details
CVE-2026-22577	Rejected reason: Not used	N/A	More Details
CVE-2026-21697	axios4go is a Go HTTP client library. Prior to version 0.6.4, a race condition vulnerability exists in the shared HTTP client configuration. The global `defaultClient` is mutated during request execution without synchronization, directly modifying the shared `http.Client`'s `Transport`, `Timeout`, and `CheckRedirect` properties. Impacted applications include that that use axios4go with concurrent requests (multiple goroutines, `GetAsync`, `PostAsync`, etc.), those where different requests use different proxy configurations, and those that handle sensitive data (authentication credentials, tokens, API keys). Version 0.6.4 fixes this issue.	N/A	More Details
CVE-2026-21427	The installers for multiple products provided by PIONEER CORPORATION contain an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with the privileges of the running installer.	N/A	More Details
CVE-2026-21857	REDAXO is a PHP-based content management system. Prior to version 5.20.2, authenticated users with backup permissions can read arbitrary files within the webroot via path traversal in the Backup addon's file export functionality. The Backup addon does not validate the `EXPDIR` POST parameter against the UI-generated allowlist of permitted directories. An attacker can supply relative paths containing `../` sequences (or even absolute paths inside the document root) to include any readable file in the generated `.tar.gz` archive. Version 5.20.2 fixes this issue.	N/A	More Details
CVE-2026-22805	Metabase is an open-source data analytics platform. Prior to 55.13, 56.3, and 57.1, self-hosted Metabase instances that allow users to create subscriptions could be potentially impacted if their Metabase is colocated with other unsecured resources. This vulnerability is fixed in 55.13, 56.3, and 57.1.	N/A	More Details
CVE-2026-22813	OpenCode is an open source AI coding agent. The markdown renderer used for LLM responses will insert arbitrary HTML into the DOM. There is no sanitization with DOMPurify or even a CSP on the web interface to prevent JavaScript execution via HTML injection. This means controlling the LLM response for a chat session gets JavaScript execution on the http://localhost:4096 origin. This vulnerability is fixed in 1.1.10.	N/A	More Details
CVE-2026-21883	Bokeh is an interactive visualization library written in Python. In versions 3.8.1 and below, if a server is configured with an allowlist (e.g., dashboard.corp), an attacker can register a domain like dashboard.corp.attacker.com (or use a subdomain if applicable) and lure a victim to visit it. The malicious site can then initiate a WebSocket connection to the vulnerable Bokeh server. Since the Origin header (e.g., http://dashboard.corp.attacker.com/) matches the allowlist according to the flawed logic, the connection is accepted. Once connected, the attacker can interact with the Bokeh server on behalf of the victim, potentially accessing sensitive data, or modifying visualizations. This issue is fixed in version 3.8.2.	N/A	More Details
CVE-2026-22829	Rejected reason: Not used	N/A	More Details
CVE-2025-9427	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lemonsoft WordPress add on allows Cross-Site Scripting (XSS).This issue affects WordPress add on: 2025.7.1.	N/A	More Details
CVE-2026-22831	Rejected reason: Not used	N/A	More Details
CVE-2025-68786	In the Linux kernel, the following vulnerability has been resolved: ksmbd: skip lock-range check on equal size to avoid size==0 underflow When size equals the current i_size (including 0), the code used to call check_lock_range(filp, i_size, size - 1, WRITE), which computes `size - 1` and can underflow for size==0. Skip the equal case.	N/A	More Details
CVE-2026-22832	Rejected reason: Not used	N/A	More Details
CVE-2026-0859	TYPO3's mail-file spool deserialization flaw lets local users with write access to the spool directory craft a malicious file that is deserialized during the mailer:spool:send command, enabling arbitrary PHP code execution on the web server. This issue affects TYPO3 CMS versions 10.0.0-10.4.54, 11.0.0-11.5.48, 12.0.0-12.4.40, 13.0.0-13.4.22 and 14.0.0-14.0.1.	N/A	More Details
CVE-	Backend users who had access to the recycler module could delete arbitrary data from any database table		

2025-59022	defined in the TCA - regardless of whether they had permission to that particular table. This allowed attackers to purge and destroy critical site data, effectively rendering the website unavailable. This issue affects TYPO3 CMS versions 10.0.0-10.4.54, 11.0.0-11.5.48, 12.0.0-12.4.40, 13.0.0-13.4.22 and 14.0.0-14.0.1.	N/A	More Details
CVE-2025-59021	Backend users with access to the redirects module and write permission on the sys_redirect table were able to read, create, and modify any redirect record without restriction to the user's own file-mounts or web-mounts. This allowed attackers to insert or alter redirects pointing to arbitrary URLs – facilitating phishing or other malicious redirect attacks. This issue affects TYPO3 CMS versions 10.0.0-10.4.54, 11.0.0-11.5.48, 12.0.0-12.4.40, 13.0.0-13.4.22 and 14.0.0-14.0.1.	N/A	More Details
CVE-2025-59020	By exploiting the defVals parameter, attackers could bypass field-level access checks during record creation in the TYPO3 backend. This gave them the ability to insert arbitrary data into prohibited exclude fields of a database table for which the user already has write permission for a reduced set of fields. This issue affects TYPO3 CMS versions 10.0.0-10.4.54, 11.0.0-11.5.48, 12.0.0-12.4.40, 13.0.0-13.4.22 and 14.0.0-14.0.1.	N/A	More Details
CVE-2026-22833	Rejected reason: Not used	N/A	More Details
CVE-2025-15346	A vulnerability in the handling of verify_mode = CERT_REQUIRED in the wolfssl Python package (wolfssl-py) causes client certificate requirements to not be fully enforced. Because the WOLFSSL_VERIFY_FAIL_IF_NO_PEER_CERT flag was not included, the behavior effectively matched CERT_OPTIONAL: a peer certificate was verified if presented, but connections were incorrectly authenticated when no client certificate was provided. This results in improper authentication, allowing attackers to bypass mutual TLS (mTLS) client authentication by omitting a client certificate during the TLS handshake. The issue affects versions up to and including 5.8.2.	N/A	More Details
CVE-2026-22834	Rejected reason: Not used	N/A	More Details
CVE-2026-22837	Rejected reason: Not used	N/A	More Details
CVE-2025-55462	A CORS misconfiguration in Eramba Community and Enterprise Editions v3.26.0 allows an attacker-controlled Origin header to be reflected in the Access-Control-Allow-Origin response along with Access-Control-Allow-Credentials: true. This permits malicious third-party websites to perform authenticated cross-origin requests against the Eramba API, including endpoints like /system-api/login and /system-api/user/me. The response includes sensitive user session data (ID, name, email, access groups), which is accessible to the attacker's JavaScript. This flaw enables full session hijack and data exfiltration without user interaction. Eramba versions 3.23.3 and earlier were tested and appear unaffected. The vulnerability is present in default installations, requiring no custom configuration.	N/A	More Details
CVE-2026-22755	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Vivotek Affected device model numbers are FD8365, FD8365v2, FD9165, FD9171, FD9187, FD9189, FD9365, FD9371, FD9381, FD9387, FD9389, FD9391,FE9180,FE9181, FE9191, FE9381, FE9382, FE9391, FE9582, IB9365, IB93587LPR, IB9371,IB9381, IB9387, IB9389, IB939,IP9165,IP9171, IP9172, IP9181, IP9191, IT9389, MA9321, MA9322, MS9321, MS9390, TB9330 (Firmware modules) allows OS Command Injection.This issue affects Affected device model numbers are FD8365, FD8365v2, FD9165, FD9171, FD9187, FD9189, FD9365, FD9371, FD9381, FD9387, FD9389, FD9391,FE9180,FE9181, FE9191, FE9381, FE9382, FE9391, FE9582, IB9365, IB93587LPR, IB9371,IB9381, IB9387, IB9389, IB939,IP9165,IP9171, IP9172, IP9181, IP9191, IT9389, MA9321, MA9322, MS9321, MS9390, TB9330: 0100a, 0106a, 0106b, 0107a, 0107b_1, 0109a, 0112a, 0113a, 0113d, 0117b, 0119e, 0120b, 0121, 0121d, 0121d_48573_1, 0122e, 0124d_48573_1, 012501, 012502, 0125c.	N/A	More Details
CVE-2025-65783	An arbitrary file upload vulnerability in the /utils/uploadFile component of Hubert Imoveis e Administracao Ltda Hub v2.0 1.27.3 allows attackers to execute arbitrary code via uploading a crafted PDF file.	N/A	More Details
CVE-2026-22214	RIOT OS versions up to and including 2026.01-devel-317 contain a stack-based buffer overflow vulnerability in the ethos utility due to missing bounds checking when processing incoming serial frame data. The vulnerability occurs in the _handle_char() function, where incoming frame bytes are appended to a fixed-size stack buffer without verifying that the current write index remains within bounds. An attacker capable of sending crafted serial or TCP-framed input can cause the current write index to exceed the buffer size, resulting in a write past the end of the stack buffer. This condition leads to memory corruption and application crash.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: fix middle attribute validation in push_nsh() action The push_nsh() action structure looks like this: OVS_ACTION_ATTR_PUSH_NSH(OVS_KEY_ATTR_NSH(OVS_NSH_KEY_ATTR_BASE,...)) The outermost OVS_ACTION_ATTR_PUSH_NSH attribute is OK'ed by the nla_for_each_nested() inside		

CVE-2025-68785	__ovs_nla_copy_actions(). The innermost OVS_NSH_KEY_ATTR_BASE/MD1/MD2 are OK'ed by the nla_for_each_nested() inside nsh_key_put_from_nlattr(). But nothing checks if the attribute in the middle is OK. We don't even check that this attribute is the OVS_KEY_ATTR_NSH. We just do a double unwrap with a pair of nla_data() calls - first time directly while calling validate_push_nsh() and the second time as part of the nla_for_each_nested() macro, which isn't safe, potentially causing invalid memory access if the size of this attribute is incorrect. The failure may not be noticed during validation due to larger netlink buffer, but cause trouble later during action execution where the buffer is allocated exactly to the size: BUG: KASAN: slab-out-of-bounds in nsh_hdr_from_nlattr+0x1dd/0x6a0 [openvswitch] Read of size 184 at addr ffff88816459a634 by task a.out/22624 CPU: 8 UID: 0 PID: 22624 6.18.0-rc7+ #115 PREEMPT(voluntary) Call Trace: <TASK> dump_stack_lvl+0x51/0x70 print_address_description.constprop.0+0x2c/0x390 kasan_report+0xdd/0x110 kasan_check_range+0x35/0x1b0 __asan_memcpy+0x20/0x60 nsh_hdr_from_nlattr+0x1dd/0x6a0 [openvswitch] push_nsh+0x82/0x120 [openvswitch] do_execute_actions+0x1405/0x2840 [openvswitch] ovs_execute_actions+0xd5/0x3b0 [openvswitch] ovs_packet_cmd_execute+0x949/0xdb0 [openvswitch] genl_family_rcv_msg_doit+0x1d6/0x2b0 genl_family_rcv_msg+0x336/0x580 genl_rcv_msg+0x9f/0x130 netlink_rcv_skb+0x11f/0x370 genl_rcv+0x24/0x40 netlink_unicast+0x73e/0xaa0 netlink_sendmsg+0x744/0xbf0 __sys_sendto+0x3d6/0x450 do_syscall_64+0x79/0x2c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e </TASK> Let's add some checks that the attribute is properly sized and it's the only one attribute inside the action. Technically, there is no real reason for OVS_KEY_ATTR_NSH to be there, as we know that we're pushing an NSH header already, it just creates extra nesting, but that's how uAPI works today. So, keeping as it is.	N/A	More Details
CVE-2025-68784	In the Linux kernel, the following vulnerability has been resolved: xfs: fix a UAF problem in xattr repair The xchk_setup_xattr_buf function can allocate a new value buffer, which means that any reference to ab->value before the call could become a dangling pointer. Fix this by moving an assignment to after the buffer setup.	N/A	More Details
CVE-2025-68783	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-mixer: us16x08: validate meter packet indices get_meter_levels_from_urb() parses the 64-byte meter packets sent by the device and fills the per-channel arrays meter_level[], comp_level[] and master_level[] in struct snd_us16x08_meter_store. Currently the function derives the channel index directly from the meter packet (MUB2(meter_urb, s) - 1) and uses it to index those arrays without validating the range. If the packet contains a negative or out-of-range channel number, the driver may write past the end of these arrays. Introduce a local channel variable and validate it before updating the arrays. We reject negative indices, limit meter_level[] and comp_level[] to SND_US16X08_MAX_CHANNELS, and guard master_level[] updates with ARRAY_SIZE(master_level).	N/A	More Details
CVE-2025-68782	In the Linux kernel, the following vulnerability has been resolved: scsi: target: Reset t_task_cdb pointer in error case If allocation of cmd->t_task_cdb fails, it remains NULL but is later dereferenced in the 'err' path. In case of error, reset NULL t_task_cdb value to point at the default fixed-size buffer. Found by Linux Verification Center (linuxtesting.org) with SVACE.	N/A	More Details
CVE-2025-68781	In the Linux kernel, the following vulnerability has been resolved: usb: phy: fsl-usb: Fix use-after-free in delayed work during device removal The delayed work item otg_event is initialized in fsl_otg_conf() and scheduled under two conditions: 1. When a host controller binds to the OTG controller. 2. When the USB ID pin state changes (cable insertion/removal). A race condition occurs when the device is removed via fsl_otg_remove(): the fsl_otg instance may be freed while the delayed work is still pending or executing. This leads to use-after-free when the work function fsl_otg_event() accesses the already freed memory. The problematic scenario: (detach thread) | (delayed work) fsl_otg_remove() | kfree(fsl_otg_dev) //FREE| fsl_otg_event() | og = container_of(...) //USE | og-> //USE Fix this by calling disable_delayed_work_sync() in fsl_otg_remove() before deallocating the fsl_otg structure. This ensures the delayed work is properly canceled and completes execution prior to memory deallocation. This bug was identified through static analysis.	N/A	More Details
CVE-2025-68780	In the Linux kernel, the following vulnerability has been resolved: sched/deadline: only set free_cpus for online runqueues Commit 16b269436b72 ("sched/deadline: Modify cpudl::free_cpus to reflect rd->online") introduced the cpudl_set/clear_freecpu functions to allow the cpu_dl::free_cpus mask to be manipulated by the deadline scheduler class rq_on/offline callbacks so the mask would also reflect this state. Commit 9659e1eeee28 ("sched/deadline: Remove cpu_active_mask from cpudl_find()") removed the check of the cpu_active_mask to save some processing on the premise that the cpudl::free_cpus mask already reflected the runqueue online state. Unfortunately, there are cases where it is possible for the cpudl_clear function to set the free_cpus bit for a CPU when the deadline runqueue is offline. When this occurs while a CPU is connected to the default root domain the flag may retain the bad state after the CPU has been unplugged. Later, a different CPU that is transitioning through the default root domain may push a deadline task to the powered down CPU when cpudl_find sees its free_cpus bit is set. If this happens the task will not have the opportunity to run. One example is outlined here: https://lore.kernel.org/lkml/20250110233010.2339521-1-opendmb@gmail.com Another occurs when the last deadline task is migrated from a CPU that has an offlined runqueue. The dequeue_task member of the deadline scheduler class will eventually call cpudl_clear and set the free_cpus bit for the CPU. This commit modifies the cpudl_clear function to be aware of the online state of the deadline runqueue so that the free_cpus mask can be updated appropriately. It is no longer necessary to manage the mask outside of the cpudl_set/clear functions so the cpudl_set/clear_freecpu functions are removed. In addition, since the free_cpus mask is now only updated under the cpudl lock the code was changed to use the non-atomic __cpumask functions.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Avoid unregistering PSP twice		

CVE-2025-68779	PSP is unregistered twice in: _mlx5e_remove -> mlx5e_psp_unregister mlx5e_nic_cleanup -> mlx5e_psp_unregister This leads to a refcount underflow in some conditions: ------------[cut here]------------ refcount_t: underflow; use-after-free. WARNING: CPU: 2 PID: 1694 at lib/refcount.c:28 refcount_warn_saturate+0xd8/0xe0 [...] mlx5e_psp_unregister+0x26/0x50 [mlx5_core] mlx5e_nic_cleanup+0x26/0x90 [mlx5_core] mlx5e_remove+0xe6/0x1f0 [mlx5_core] auxiliary_bus_remove+0x18/0x30 device_release_driver_internal+0x194/0x1f0 bus_remove_device+0xc6/0x130 device_del+0x159/0x3c0 mlx5_rescan_drivers_locked+0xbc/0x2a0 [mlx5_core] [...] Do not directly remove psp from the _mlx5e_remove path, the PSP cleanup happens as part of profile cleanup.	N/A	More Details
CVE-2025-68778	In the Linux kernel, the following vulnerability has been resolved: btrfs: don't log conflicting inode if it's a dir moved in the current transaction We can't log a conflicting inode if it's a directory and it was moved from one parent directory to another parent directory in the current transaction, as this can result an attempt to have a directory with two hard links during log replay, one for the old parent directory and another for the new parent directory. The following scenario triggers that issue: 1) We have directories "dir1" and "dir2" created in a past transaction. Directory "dir1" has inode A as its parent directory; 2) We move "dir1" to some other directory; 3) We create a file with the name "dir1" in directory inode A; 4) We fsync the new file. This results in logging the inode of the new file and the inode for the directory "dir1" that was previously moved in the current transaction. So the log tree has the INODE_REF item for the new location of "dir1"; 5) We move the new file to some other directory. This results in updating the log tree to included the new INODE_REF for the new location of the file and removes the INODE_REF for the old location. This happens during the rename when we call btrfs_log_new_name(); 6) We fsync the file, and that persists the log tree changes done in the previous step (btrfs_log_new_name() only updates the log tree in memory); 7) We have a power failure; 8) Next time the fs is mounted, log replay happens and when processing the inode for directory "dir1" we find a new INODE_REF and add that link, but we don't remove the old link of the inode since we have not logged the old parent directory of the directory inode "dir1". As a result after log replay finishes when we trigger writeback of the subvolume tree's extent buffers, the tree check will detect that we have a directory a hard link count of 2 and we get a mount failure. The errors and stack traces reported in dmesg/syslog are like this: [3845.729764] BTRFS info (device dm-0): start tree-log replay [3845.730304] page: refcount:3 mapcount:0 mapping:000000005c8a3027 index:0x1d00 pfn:0x11510c [3845.731236] memcg:ffff9264c02f4e00 [3845.731751] aops:btree_aops [btrfs] ino:1 [3845.732300] flags: 0x17fffc00000400a(uptodate|private|writeback|node=0|zone=2|lastcpupid=0x1ffff) [3845.733346] raw: 017fffc00000400a 0000000000000000 dead000000000122 ffff9264d978aea8 [3845.734265] raw: 0000000000001d00 ffff92650e6d4738 00000003ffffffff ffff9264c02f4e00 [3845.735305] page dumped because: eb page dump [3845.735981] BTRFS critical (device dm-0): corrupt leaf: root=5 block=30408704 slot=6 ino=257, invalid nlink: has 2 expect no more than 1 for dir [3845.737786] BTRFS info (device dm-0): leaf 30408704 gen 10 total ptrs 17 free space 14881 owner 5 [3845.737789] BTRFS info (device dm-0): refs 4 lock_owner 0 current 30701 [3845.737792] item 0 key (256 INODE_ITEM 0) itemoff 16123 itemsize 160 [3845.737794] inode generation 3 transid 9 size 16 nbytes 16384 [3845.737795] block group 0 mode 40755 links 1 uid 0 gid 0 [3845.737797] rdev 0 sequence 2 flags 0x0 [3845.737798] atime 1764259517.0 [3845.737800] ctime 1764259517.572889464 [3845.737801] mtime 1764259517.572889464 [3845.737802] otime 1764259517.0 [3845.737803] item 1 key (256 INODE_REF 256) itemoff 16111 itemsize 12 [3845.737805] index 0 name_len 2 [3845.737807] item 2 key (256 DIR_ITEM 2363071922) itemoff 16077 itemsize 34 [3845.737808] location key (257 1 0) type 2 [3845.737810] transid 9 data_len 0 name_len 4 [3845.737811] item 3 key (256 DIR_ITEM 2676584006) itemoff 16043 itemsize 34 [3845.737813] location key (258 1 0) type 2 [3845.737814] transid 9 data_len 0 name_len 4 [3845.737815] item 4 key (256 DIR_INDEX 2) itemoff 16009 itemsize 34 [3845.737816] location key (257 1 0) type 2 [---truncated---	N/A	More Details
CVE-2025-68777	In the Linux kernel, the following vulnerability has been resolved: Input: ti_am335x_tsc - fix off-by-one error in wire_order validation The current validation 'wire_order[i] > ARRAY_SIZE(config_pins)' allows wire_order[i] to equal ARRAY_SIZE(config_pins), which causes out-of-bounds access when used as index in 'config_pins[wire_order[i]]'. Since config_pins has 4 elements (indices 0-3), the valid range for wire_order should be 0-3. Fix the off-by-one error by using >= instead of > in the validation check.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: net/hsr: fix NULL pointer dereference in prp_get_untagged_frame() prp_get_untagged_frame() calls __pskb_copy() to create frame->skb_std but doesn't check if the allocation failed. If __pskb_copy() returns NULL, skb_clone() is called with a NULL pointer, causing a crash: Oops: general protection fault, probably for non-canonical address 0xdfffffc000000000f: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000078-0x000000000000007f] CPU: 0 UID: 0 PID: 5625 Comm: syz.1.18 Not tainted 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:skb_clone+0xd7/0x3a0 net/core/skbuff.c:2041 Code: 03 42 80 3c 20 00 74 08 4c 89 f7 e8 23 29 05 f9 49 83 3e 00 0f 85 a0 01 00 00 e8 94 dd 9d f8 48 8d 6b 7e 49 89 ee 49 c1 ee 03 <43> 0f b6 04 26 84 c0 0f 85 d1 01 00 00 44 0f b6 7d 00 41 83 e7 0c RSP: 0018:ffffc9000d00f200 EFLAGS: 00010207 RAX: ffffffff892235a1 RBX: 0000000000000000 RCX: ffff88803372a480 RDX: 0000000000000000 RSI: 0000000000000820 RDI: 0000000000000000 RBP: 000000000000007e R08: ffffffff8f7d0f77 R09: 1ffffffff1efa1ee R10: dffffc0000000000 R11: fffffbfff1efa1ef R12: dffffc0000000000 R13: 0000000000000820 R14: 000000000000000f R15: ffff88805144cc00 FS: 0000555557f6d500(0000) GS:ffff88808d72f000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000555581d35808 CR3: 000000005040e000 CR4: 0000000000352ef0 Call Trace: <TASK> hsr_forward_do net/hsr/hsr_forward.c:-1 [inline] hsr_forward_skb+0x1013/0x2860	N/A	More

68776	net/hsr/hsr_forward.c:741 hsr_handle_frame+0x6ce/0xa70 net/hsr/hsr_slave.c:84 __netif_receive_skb_core+0x10b9/0x4380 net/core/dev.c:5966 __netif_receive_skb_one_core net/core/dev.c:6077 [inline] __netif_receive_skb+0x72/0x380 net/core/dev.c:6192 netif_receive_skb_internal net/core/dev.c:6278 [inline] netif_receive_skb+0x1cb/0x790 net/core/dev.c:6337 tun_rx_batched+0x1b9/0x730 drivers/net/tun.c:1485 tun_get_user+0x2b65/0x3e90 drivers/net/tun.c:1953 tun_chr_write_iter+0x113/0x200 drivers/net/tun.c:1999 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x5c9/0xb30 fs/read_write.c:686 ksys_write+0x145/0x250 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f0449f8e1ff Code: 89 54 24 18 48 89 74 24 10 89 7c 24 08 e8 f9 92 02 00 48 8b 54 24 18 48 8b 74 24 10 41 89 c0 8b 7c 24 08 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 31 44 89 c7 48 89 44 24 08 e8 4c 93 02 00 48 RSP: 002b:00007ffd7ad94c90 EFLAGS: 00000293 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00007f044a1e5fa0 RCX: 00007f0449f8e1ff RDX: 000000000000003e RSI: 0000200000000500 RDI: 00000000000000c8 RBP: 00007ffd7ad94d20 R08: 0000000000000000 R09: 0000000000000000 R10: 000000000000003e R11: 0000000000000293 R12: 0000000000000001 R13: 00007f044a1e5fa0 R14: 00007f044a1e5fa0 R15: 0000000000000003 </TASK> Add a NULL check immediately after __pskb_copy() to handle allocation failures gracefully.		Details
CVE-2025-68775	In the Linux kernel, the following vulnerability has been resolved: net/handshake: duplicate handshake cancellations leak socket When a handshake request is cancelled it is removed from the handshake_net->hn_requests list, but it is still present in the handshake_rhashtbl until it is destroyed. If a second cancellation request arrives for the same handshake request, then remove_pending() will return false... and assuming HANDSHAKE_F_REQ_COMPLETED isn't set in req->hr_flags, we'll continue processing through the out_true label, where we put another reference on the sock and a refcount underflow occurs. This can happen for example if a handshake times out - particularly if the SUNRPC client sends the AUTH_TLS probe to the server but doesn't follow it up with the ClientHello due to a problem with tlshd. When the timeout is hit on the server, the server will send a FIN, which triggers a cancellation request via xs_reset_transport(). When the timeout is hit on the client, another cancellation request happens via xs_tls_handshake_sync(). Add a test_and_set_bit(HANDSHAKE_F_REQ_COMPLETED) in the pending cancel path so duplicate cancels can be detected.	N/A	More Details
CVE-2025-68774	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix missing hfs_bnode_get() in __hfs_bnode_create When sync() and link() are called concurrently, both threads may enter hfs_bnode_find() without finding the node in the hash table and proceed to create it. Thread A: hfsplus_write_inode() -> hfsplus_write_system_inode() -> hfs_btree_write() -> hfs_bnode_find(tree, 0) -> __hfs_bnode_create(tree, 0) Thread B: hfsplus_create_cat() -> hfs_brec_insert() -> hfs_bnode_split() -> hfs_bmap_alloc() -> hfs_bnode_find(tree, 0) -> __hfs_bnode_create(tree, 0) In this case, thread A creates the bnode, sets refcnt=1, and hashes it. Thread B also tries to create the same bnode, notices it has already been inserted, drops its own instance, and uses the hashed one without getting the node. ``` node2 = hfs_bnode_findhash(tree, cnid); if (!node2) { <- Thread A hash = hfs_bnode_hash(cnid); node->next_hash = tree->node_hash[hash]; tree->node_hash[hash] = node; tree->node_hash_cnt++; } else { <- Thread B spin_unlock(&tree->hash_lock); kfree(node); wait_event(node2->lock_wq, !test_bit(HFS_BNODE_NEW, &node2->flags)); return node2; } ``` However, hfs_bnode_find() requires each call to take a reference. Here both threads end up setting refcnt=1. When they later put the node, this triggers: BUG_ON(!atomic_read(&node->refcnt)) In this scenario, Thread B in fact finds the node in the hash table rather than creating a new one, and thus must take a reference. Fix this by calling hfs_bnode_get() when reusing a bnode newly created by another thread to ensure the refcount is updated correctly. A similar bug was fixed in HFS long ago in commit a9dc087fd3c4 ("fix missing hfs_bnode_get() in __hfs_bnode_create") but the same issue remained in HFS+ until now.	N/A	More Details
CVE-2025-68773	In the Linux kernel, the following vulnerability has been resolved: spi: fsl-cpm: Check length parity before switching to 16 bit mode Commit fc96ec826bce ("spi: fsl-cpm: Use 16 bit mode for large transfers with even size") failed to make sure that the size is really even before switching to 16 bit mode. Until recently the problem went unnoticed because kernfs uses a pre-allocated bounce buffer of size PAGE_SIZE for reading EEPROM. But commit 8ad6249c51d0 ("eeprom: at25: convert to spi-mem API") introduced an additional dynamically allocated bounce buffer whose size is exactly the size of the transfer, leading to a buffer overrun in the fsl-cpm driver when that size is odd. Add the missing length parity verification and remain in 8 bit mode when the length is not even.	N/A	More Details
CVE-2025-68772	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid updating compression context during writeback Bai, Shuangpeng <sjb7183@psu.edu> reported a bug as below: Oops: divide error: 0000 [#1] SMP KASAN PTI CPU: 0 UID: 0 PID: 11441 Comm: syz.0.46 Not tainted 6.17.0 #1 PREEMPT(full) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:f2fs_all_cluster_page_ready+0x106/0x550 fs/f2fs/compress.c:857 Call Trace: <TASK> f2fs_write_cache_pages fs/f2fs/data.c:3078 [inline] __f2fs_write_data_pages fs/f2fs/data.c:3290 [inline] f2fs_write_data_pages+0x1c19/0x3600 fs/f2fs/data.c:3317 do_writepages+0x38e/0x640 mm/page-writeback.c:2634 filemap_fdatawrite_wbc mm/filemap.c:386 [inline] __filemap_fdatawrite_range mm/filemap.c:419 [inline] file_write_and_wait_range+0x2ba/0x3e0 mm/filemap.c:794 f2fs_do_sync_file+0x6e6/0x1b00 fs/f2fs/file.c:294 generic_write_sync include/linux/fs.h:3043 [inline] f2fs_file_write_iter+0x76e/0x2700 fs/f2fs/file.c:5259 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x7e9/0xe00 fs/read_write.c:686 ksys_write+0x19d/0x2d0 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xf7/0x470 arch/x86/entry/syscall_64.c:94	N/A	More Details

	entry_SYSCALL_64_after_hwframe+0x77/0x7f The bug was triggered w/ below race condition: fsync setattr ioctl - f2fs_do_sync_file - file_write_and_wait_range - f2fs_write_cache_pages : inode is non-compressed : cc.cluster_size = F2FS_I(inode)->i_cluster_size = 0 - tag_pages_for_writeback - f2fs_setattr - truncate_setsize - f2fs_truncate - f2fs_fileattr_set - f2fs_setflags_common - set_compress_context : F2FS_I(inode)->i_cluster_size = 4 : set_inode_flag(inode, FI_COMPRESSED_FILE) - f2fs_compressed_file : return true - f2fs_all_cluster_page_ready : "pgidx % cc->cluster_size" trigger dividing 0 issue Let's change as below to fix this issue: - introduce a new atomic type variable .writeback in structure f2fs_inode_info to track the number of threads which calling f2fs_write_cache_pages(). - use .i_sem lock to protect .writeback update. - check .writeback before update compression context in f2fs_setflags_common() to avoid race w/ ->writepages.		
CVE-2025-68771	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix kernel BUG in ocfs2_find_victim_chain syzbot reported a kernel BUG in ocfs2_find_victim_chain() because the `cl_next_free_rec` field of the allocation chain list (next free slot in the chain list) is 0, triggring the BUG_ON(!cl->cl_next_free_rec) condition in ocfs2_find_victim_chain() and panicking the kernel. To fix this, an if condition is introduced in ocfs2_claim_suballoc_bits(), just before calling ocfs2_find_victim_chain(), the code block in it being executed when either of the following conditions is true: 1. `cl_next_free_rec` is equal to 0, indicating that there are no free chains in the allocation chain list 2. `cl_next_free_rec` is greater than `cl_count` (the total number of chains in the allocation chain list) Either of them being true is indicative of the fact that there are no chains left for usage. This is addressed using ocfs2_error(), which prints the error log for debugging purposes, rather than panicking the kernel.	N/A	More Details
CVE-2025-68770	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Fix XDP_TX path For XDP_TX action in bnxt_rx_xdp(), clearing of the event flags is not correct. __bnxt_poll_work() -> bnxt_rx_pkt() -> bnxt_rx_xdp() may be looping within NAPI and some event flags may be set in earlier iterations. In particular, if BNXT_TX_EVENT is set earlier indicating some XDP_TX packets are ready and pending, it will be cleared if it is XDP_TX action again. Normally, we will set BNXT_TX_EVENT again when we successfully call __bnxt_xmit_xdp(). But if the TX ring has no more room, the flag will not be set. This will cause the TX producer to be ahead but the driver will not hit the TX doorbell. For multi-buf XDP_TX, there is no need to clear the event flags and set BNXT_AGG_EVENT. The BNXT_AGG_EVENT flag should have been set earlier in bnxt_rx_pkt(). The visible symptom of this is that the RX ring associated with the TX XDP ring will eventually become empty and all packets will be dropped. Because this condition will cause the driver to not refill the RX ring seeing that the TX ring has forever pending XDP_TX packets. The fix is to only clear BNXT_RX_EVENT when we have successfully called __bnxt_xmit_xdp().	N/A	More Details
CVE-2025-68769	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix return value of f2fs_recover_fsync_data() With below scripts, it will trigger panic in f2fs: mkfs.f2fs -f /dev/vdd mount /dev/vdd /mnt/f2fs touch /mnt/f2fs/foo sync echo 111 >> /mnt/f2fs/foo f2fs_io fsync /mnt/f2fs/foo f2fs_io shutdown 2 /mnt/f2fs umount /mnt/f2fs mount -o ro,norecovery /dev/vdd /mnt/f2fs or mount -o ro,disable_roll_forward /dev/vdd /mnt/f2fs F2FS-fs (vdd): f2fs_recover_fsync_data: recovery fsync data, check_only: 0 F2FS-fs (vdd): Mounted with checkpoint version = 7f5c361f F2FS-fs (vdd): Stopped filesystem due to reason: 0 F2FS-fs (vdd): f2fs_recover_fsync_data: recovery fsync data, check_only: 1 Filesystem f2fs get_tree() didn't set fc->root, returned 1 ------------[cut here]------------ kernel BUG at fs/super.c:1761! Oops: invalid opcode: 0000 [#1] SMP PTI CPU: 3 UID: 0 PID: 722 Comm: mount Not tainted 6.18.0-rc2+ #721 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:vfs_get_tree.cold+0x18/0x1a Call Trace: <TASK> fc_mount+0x13/0xa0 path_mount+0x34e/0xc50 __x64_sys_mount+0x121/0x150 do_syscall_64+0x84/0x800 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fa6cc126cfe The root cause is we missed to handle error number returned from f2fs_recover_fsync_data() when mounting image w/ ro,norecovery or ro,disable_roll_forward mount option, result in returning a positive error number to vfs_get_tree(), fix it.	N/A	More Details
CVE-2025-68768	In the Linux kernel, the following vulnerability has been resolved: inet: frags: flush pending skbs in fqdir_pre_exit() We have been seeing occasional deadlocks on pernet_ops_rwsem since September in NIPA. The stuck task was usually modprobe (often loading a driver like ipvlan), trying to take the lock as a Writer. lockdep does not track readers for rwsems so the read wasn't obvious from the reports. On closer inspection the Reader holding the lock was conntrack looping forever in nf_conntrack_cleanup_net_list(). Based on past experience with occasional NIPA crashes I looked thru the tests which run before the crash and noticed that the crash follows ip_defrag.sh. An immediate red flag. Scouring thru (de)fragmentation queues reveals skbs sitting around, holding conntrack references. The problem is that since conntrack depends on nf_defrag_ipv6, nf_defrag_ipv6 will load first. Since nf_defrag_ipv6 loads first its netns exit hooks run _after_ conntrack's netns exit hook. Flush all fragment queue SKBs during fqdir_pre_exit() to release conntrack references before conntrack cleanup runs. Also flush the queues in timer expiry handlers when they discover fqdir->dead is set, in case packet sneaks in while we're running the pre_exit flush. The commit under Fixes is not exactly the culprit, but I think previously the timer firing would eventually unblock the spinning conntrack.	N/A	More Details
CVE-2025-68767	In the Linux kernel, the following vulnerability has been resolved: hfsplus: Verify inode mode when loading from disk syzbot is reporting that S_IFMT bits of inode->i_mode can become bogus when the S_IFMT bits of the 16bits "mode" field loaded from disk are corrupted. According to [1], the permissions field was treated as reserved in Mac OS 8 and 9. According to [2], the reserved field was explicitly initialized with 0, and that field must remain 0 as long as reserved. Therefore, when the "mode" field is not 0 (i.e. no longer reserved), the file must be S_IFDIR if dir == 1, and the file must be one of S_IFREG/S_IFLNK/S_IFCHR/ S_IFBLK/S_IFIFO/S_IFSOCK if dir == 0.	N/A	More Details

CVE-2025-71065	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid potential deadlock As Jiaming Zhang and syzbot reported, there is potential deadlock in f2fs as below: Chain exists of: &sbi->cp_rwsem --> fs_reclaim --> sb_internal#2 Possible unsafe locking scenario: CPU0 CPU1 ---- ---- rlock(sb_internal#2); lock(fs_reclaim); lock(sb_internal#2); rlock(&sbi->cp_rwsem); *** DEADLOCK *** 3 locks held by kswapd0/73: #0: ffffffff8e247a40 (fs_reclaim){+.+.}-{0:0}, at: balance_pgdat mm/vmscan.c:7015 [inline] #0: ffffffff8e247a40 (fs_reclaim){+.+.}-{0:0}, at: kswapd+0x951/0x2800 mm/vmscan.c:7389 #1: ffff8880118400e0 (&type->s_umount_key#50){.+.+}-{4:4}, at: super_trylock_shared fs/super.c:562 [inline] #1: ffff8880118400e0 (&type->s_umount_key#50){.+.+}-{4:4}, at: super_cache_scan+0x91/0x4b0 fs/super.c:197 #2: ffff888011840610 (sb_internal#2){.+.+}-{0:0}, at: f2fs_evict_inode+0x8d9/0x1b60 fs/f2fs/inode.c:890 stack backtrace: CPU: 0 UID: 0 PID: 73 Comm: kswapd0 Not tainted 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 Call Trace: <TASK> dump_stack_lvl+0x189/0x250 lib/dump_stack.c:120 print_circular_bug+0x2ee/0x310 kernel/locking/lockdep.c:2043 check_noncircular+0x134/0x160 kernel/locking/lockdep.c:2175 check_prev_add kernel/locking/lockdep.c:3165 [inline] check_prevs_add kernel/locking/lockdep.c:3284 [inline] validate_chain+0xb9b/0x2140 kernel/locking/lockdep.c:3908 __lock_acquire+0xab9/0xd20 kernel/locking/lockdep.c:5237 lock_acquire+0x120/0x360 kernel/locking/lockdep.c:5868 down_read+0x46/0x2e0 kernel/locking/rwsem.c:1537 f2fs_down_read fs/f2fs/f2fs.h:2278 [inline] f2fs_lock_op fs/f2fs/f2fs.h:2357 [inline] f2fs_do_truncate_blocks+0x21c/0x10c0 fs/f2fs/file.c:791 f2fs_truncate_blocks+0x10a/0x300 fs/f2fs/file.c:867 f2fs_truncate+0x489/0x7c0 fs/f2fs/file.c:925 f2fs_evict_inode+0x9f2/0x1b60 fs/f2fs/inode.c:897 evict+0x504/0x9c0 fs/inode.c:810 f2fs_evict_inode+0x1dc/0x1b60 fs/f2fs/inode.c:853 evict+0x504/0x9c0 fs/inode.c:810 dispose_list fs/inode.c:852 [inline] prune_icache_sb+0x21b/0x2c0 fs/inode.c:1000 super_cache_scan+0x39b/0x4b0 fs/super.c:224 do_shrink_slab+0x6ef/0x1110 mm/shrinker.c:437 shrink_slab_memcg mm/shrinker.c:550 [inline] shrink_slab+0x7ef/0x10d0 mm/shrinker.c:628 shrink_one+0x28a/0x7c0 mm/vmscan.c:4955 shrink_many mm/vmscan.c:5016 [inline] lru_gen_shrink_node mm/vmscan.c:5094 [inline] shrink_node+0x315d/0x3780 mm/vmscan.c:6081 kswapd_shrink_node mm/vmscan.c:6941 [inline] balance_pgdat mm/vmscan.c:7124 [inline] kswapd+0x147c/0x2800 mm/vmscan.c:7389 kthread+0x70e/0x8a0 kernel/kthread.c:463 ret_from_fork+0x4bc/0x870 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> The root cause is deadlock among four locks as below: kswapd - fs_reclaim --- Lock A - shrink_one - evict - f2fs_evict_inode - sb_start_intwrite --- Lock B - iput - evict - f2fs_evict_inode - sb_start_intwrite --- Lock B - f2fs_truncate - f2fs_truncate_blocks - f2fs_do_truncate_blocks - f2fs_lock_op --- Lock C ioctl - f2fs_ioc_commit_atomic_write - f2fs_lock_op --- Lock C - __f2fs_commit_atomic_write - __replace_atomic_write_block - f2fs_get_dnode_of_data - __get_node_folio - f2fs_check_nid_range - f2fs_handle_error - f2fs_record_errors - f2fs_down_write --- Lock D open - do_open - do_truncate - security_inode_need_killpriv - f2fs_getxattr - lookup_all_xattrs - f2fs_handle_error - f2fs_record_errors - f2fs_down_write --- Lock D - f2fs_commit_super - read_mapping_folio - filemap_alloc_folio_noprof - prepare_alloc_pages - fs_reclaim_acquire --- Lock A In order to a ---truncated---	N/A	More Details
CVE-2025-71067	In the Linux kernel, the following vulnerability has been resolved: ntfs: set dummy blocksize to read boot_block when mounting When mounting, sb->s_blocksize is used to read the boot_block without being defined or validated. Set a dummy blocksize before attempting to read the boot_block. The issue can be triggered with the following syz reproducer: mkdirat(0xffffffffffffff9c, &(0x7f0000000080)='./file1\x00', 0x0) r4 = openat$nullb(0xffffffffffffff9c, &(0x7f0000000040), 0x121403, 0x0) ioctl$FS_IOC_SETFLAGS(r4, 0x40081271, &(0x7f0000000980)=0x4000) mount(&(0x7f0000000140)=@nullb, &(0x7f0000000040)='./cgroup\x00', &(0x7f0000000000)='ntfs3\x00', 0x2208004, 0x0) syz_clone(0x88200200, 0x0, 0x0, 0x0, 0x0, 0x0) Here, the ioctl sets the bdev block size to 16384. During mount, get_tree_bdev_flags() calls sb_set_blocksize(sb, block_size(bdev)), but since block_size(bdev) > PAGE_SIZE, sb_set_blocksize() leaves sb->s_blocksize at zero. Later, ntfs_init_from_boot() attempts to read the boot_block while sb->s_blocksize is still zero, which triggers the bug. [almaz.alexandrovich@paragon-software.com: changed comment style, added return value handling]	N/A	More Details
CVE-2026-22544	An attacker with a network connection could detect credentials in clear text.	N/A	More Details
CVE-2026-22185	OpenLDAP Lightning Memory-Mapped Database (LMDB) versions up to and including 0.9.14, prior to commit 8e1fda8, contain a heap buffer underflow in the readline() function of mdb_load. When processing malformed input containing an embedded NUL byte, an unsigned offset calculation can underflow and cause an out-of-bounds read of one byte before the allocated heap buffer. This can cause mdb_load to crash, leading to a limited denial-of-service condition.	N/A	More Details
CVE-2026-22785	orval generates type-safe JS clients (TypeScript) from any valid OpenAPI v3 or Swagger v2 specification. Prior to 7.18.0, the MCP server generation logic relies on string manipulation that incorporates the summary field from the OpenAPI specification without proper validation or escaping. This allows an attacker to "break out" of the string literal and inject arbitrary code. This vulnerability is fixed in 7.18.0.	N/A	More Details
CVE-2026-22539	As the service interaction is performed without authentication, an attacker with some knowledge of the protocol could obtain information about the charger via OCPP v1.6.	N/A	More Details

CVE-2026-22579	Rejected reason: Not used	N/A	More Details
CVE-2025-12420	A vulnerability has been identified in the ServiceNow AI Platform that could enable an unauthenticated user to impersonate another user and perform the operations that the impersonated user is entitled to perform. ServiceNow has addressed this vulnerability by deploying a relevant security update to hosted instances in October 2025. Security updates have also been provided to ServiceNow self-hosted customers, partners, and hosted customers with unique configurations. Additionally, the vulnerability is addressed in the listed Store App versions. We recommend that customers promptly apply an appropriate security update or upgrade if they have not already done so.	N/A	More Details
CVE-2026-22786	Gin-vue-admin is a backstage management system based on vue and gin. Gin-vue-admin <= v2.8.7 has a path traversal vulnerability in the breakpoint resume upload functionality. Attacker can upload any files on any directory. In the breakpoint_continue.go file, the MakeFile function accepts a fileName parameter through the /fileUploadAndDownload/breakpointContinueFinish API endpoint and directly concatenates it with the base directory path (./fileDir/) using os.OpenFile() without any validation for directory traversal sequences (e.g., ../). An attacker with file upload privileges could exploit this vulnerability.	N/A	More Details
CVE-2025-68705	RustFS is a distributed object storage system built in Rust. In versions 1.0.0-alpha.13 to 1.0.0-alpha.78, RustFS contains a path traversal vulnerability in the /rustfs/rpc/read_file_stream endpoint. This issue has been patched in version 1.0.0-alpha.79.	N/A	More Details
CVE-2025-69255	RustFS is a distributed object storage system built in Rust. In versions 1.0.0-alpha.13 to 1.0.0-alpha.77, a malformed gRPC GetMetrics request causes get_metrics to unwrap() failed deserialization of metric_type/opts, panicking the handler thread and enabling remote denial of service of the metrics endpoint. This issue has been patched in version 1.0.0-alpha.78.	N/A	More Details
CVE-2026-22184	zlib versions up to and including 1.3.1.2 contain a global buffer overflow in the untgz utility. The TGZfname() function copies an attacker-supplied archive name from argv[] into a fixed-size 1024-byte static global buffer using an unbounded strcpy() call without length validation. Supplying an archive name longer than 1024 bytes results in an out-of-bounds write that can lead to memory corruption, denial of service, and potentially code execution depending on compiler, build flags, architecture, and memory layout. The overflow occurs prior to any archive parsing or validation.	N/A	More Details
CVE-2026-22578	Rejected reason: Not used	N/A	More Details
CVE-2026-22186	Bio-Formats versions up to and including 8.3.0 contain an XML External Entity (XXE) vulnerability in the Leica Microsystems metadata parsing component (e.g., XLEF). The parser uses an insecurely configured DocumentBuilderFactory when processing Leica XML-based metadata files, allowing external entity expansion and external DTD loading. A crafted metadata file can trigger outbound network requests (SSRF), access local system resources where readable, or cause a denial of service during XML parsing.	N/A	More Details
CVE-2026-22781	TinyWeb is a web server (HTTP, HTTPS) written in Delphi for Win32. TinyWeb HTTP Server before version 1.98 is vulnerable to OS command injection via CGI ISINDEX-style query parameters. The query parameters are passed as command-line arguments to the CGI executable via Windows CreateProcess(). An unauthenticated remote attacker can execute arbitrary commands on the server by injecting Windows shell metacharacters into HTTP requests. This vulnerability is fixed in 1.98.	N/A	More Details
CVE-2026-22187	Bio-Formats versions up to and including 8.3.0 perform unsafe Java deserialization of attacker-controlled memoization cache files (.bfmemo) during image processing. The loci.formats.Memoizer class automatically loads and deserializes memo files associated with images without validation, integrity checks, or trust enforcement. An attacker who can supply a crafted .bfmemo file alongside an image can trigger deserialization of untrusted data, which may result in denial of service, logic manipulation, or potentially remote code execution in environments where suitable gadget chains are present on the classpath.	N/A	More Details
CVE-2026-22799	Emlog is an open source website building system. emlog v2.6.1 and earlier exposes a REST API endpoint (/index.php?rest-api=upload) for media file uploads. The endpoint fails to implement proper validation of file types, extensions, and content, allowing authenticated attackers (with a valid API key or admin session cookie) to upload arbitrary files (including malicious PHP scripts) to the server. An attacker can obtain the API key either by gaining administrator access to enable the REST API setting, or via information disclosure vulnerabilities in the application. Once uploaded, the malicious PHP file can be executed to gain remote code execution (RCE) on the target server, leading to full server compromise.	N/A	More Details
CVE-2025-	The Report Builder component of the application stores user input directly in a web page and displays it to other users, which raised concerns about a possible Cross-Site Scripting (XSS) attack. Proper management of this functionality helps ensure a secure and seamless user experience. Although the user input is not validated in the report creation, these scripts are not executed when the report is run by end users. The script is executed when the report is modified through the report builder by a user with edit permissions. The Report Builder is part of the WebConsole. The WebConsole package is currently end of life, and is no longer	N/A	More Details

12776	maintained. We strongly recommend against installing or using it in any production environment. However, if you choose to install it, for example, to access functionality like the Report Builder, it must be deployed within a fully isolated network that has no access to sensitive data or internet connectivity. This is a critical security precaution, as the retired package may contain unpatched vulnerabilities and is no longer supported with updates or fixes.		
CVE-2025-10865	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause mismanagement of reference counting to cause a potential use after free. Improper reference counting on an internal resource caused scenario where potential for use after free was present.	N/A	More Details
CVE-2024-14021	LlamaIndex (run-llama/llama_index) versions up to and including 0.11.6 contain an unsafe deserialization vulnerability in BGEM3Index.load_from_disk() in llama_index/indices/managed/bge_m3/base.py. The function uses pickle.load() to deserialize multi_embed_store.pkl from a user-supplied persist_dir without validation. An attacker who can provide a crafted persist directory containing a malicious pickle file can trigger arbitrary code execution when the victim loads the index from disk.	N/A	More Details
CVE-2025-68707	An authentication bypass vulnerability in the Tongyu AX1800 Wi-Fi 6 Router with firmware 1.0.0 allows unauthenticated network-adjacent attackers to perform arbitrary configuration changes without providing credentials, as long as a valid admin session is active. This can result in full compromise of the device (i.e., via unauthenticated access to /boaform/formSaveConfig and /boaform/admin endpoints).	N/A	More Details
CVE-2025-65784	Insecure permissions in Hubert Imoveis e Administracao Ltda Hub v2.0 1.27.3 allows authenticated attackers with low-level privileges to access other users' information via a crafted API request.	N/A	More Details
CVE-2025-62182	Pega Customer Service Framework versions 8.7.0 through 25.1.0 are affected by a Unrestricted file upload vulnerability, where a privileged user could potentially upload a malicious file.	N/A	More Details
CVE-2026-21441	urllib3 is an HTTP client library for Python. urllib3's streaming API is designed for the efficient handling of large HTTP responses by reading the content in chunks, rather than loading the entire response body into memory at once. urllib3 can perform decoding or decompression based on the HTTP `Content-Encoding` header (e.g., `gzip`, `deflate`, `br`, or `zstd`). When using the streaming API, the library decompresses only the necessary bytes, enabling partial content consumption. Starting in version 1.22 and prior to version 2.6.3, for HTTP redirect responses, the library would read the entire response body to drain the connection and decompress the content unnecessarily. This decompression occurred even before any read methods were called, and configured read limits did not restrict the amount of decompressed data. As a result, there was no safeguard against decompression bombs. A malicious server could exploit this to trigger excessive resource consumption on the client. Applications and libraries are affected when they stream content from untrusted sources by setting `preload_content=False` when they do not disable redirects. Users should upgrade to at least urllib3 v2.6.3, in which the library does not decode content of redirect responses when `preload_content=False`. If upgrading is not immediately possible, disable redirects by setting `redirect=False` for requests to untrusted source.	N/A	More Details
CVE-2026-22784	Lychee is a free, open-source photo-management tool. Prior to 7.1.0, an authorization vulnerability exists in Lychee's album password unlock functionality that allows users to gain possibly unauthorized access to other users' password-protected albums. When a user unlocks a password-protected public album, the system automatically unlocks ALL other public albums that share the same password, resulting in a complete authorization bypass. This vulnerability is fixed in 7.1.0.	N/A	More Details
CVE-2026-22776	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to version 0.30.1, a Denial of Service (DoS) vulnerability exists in cpp-httplib due to the unsafe handling of compressed HTTP request bodies (Content-Encoding: gzip, br, etc.). The library validates the payload_max_length against the compressed data size received from the network, but does not limit the size of the decompressed data stored in memory.	N/A	More Details
CVE-2025-71068	In the Linux kernel, the following vulnerability has been resolved: svcrdma: bound check rq_pages index in inline path svc_rdma_copy_inline_range indexed rqstp->rq_pages[rc_curpage] without verifying rc_curpage stays within the allocated page array. Add guards before the first use and after advancing to a new page.	N/A	More Details
CVE-2025-41003	Imaster's Patient Record Management System contains a stored Cross-Site Scripting (XSS) vulnerability in the endpoint '/projects/hospital/admin/edit_patient.php'. By injecting a malicious script into the 'firstname' parameter, the JavaScript code is stored and executed every time a user accesses the patient list, allowing an attacker to execute arbitrary JavaScript in a victim's browser.	N/A	More Details
CVE-2025-69274	Authorization Bypass Through User-Controlled Key vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Privilege Escalation.This issue affects DX NetOps Spectrum: 24.3.10 and earlier.	N/A	More Details
CVE-2025-	Knowage is an open source analytics and business intelligence suite. Prior to version 8.1.37, there is a blind server-side request forgery vulnerability. The vulnerability allows attackers to send requests to arbitrary hosts/paths. Since the attacker is not able to read the response, the impact of this vulnerability is limited.	N/A	More Details

58441	However, an attacker should be able to leverage this vulnerability to scan the internal network. This issue has been patched in version 8.1.37.		
CVE-2025-69275	Dependency on Vulnerable Third-Party Component vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows DOM-Based XSS.This issue affects DX NetOps Spectrum: 24.3.9 and earlier.	N/A	More Details
CVE-2025-69276	Deserialization of Untrusted Data vulnerability in Broadcom DX NetOps Spectrum on Windows, Linux allows Object Injection.This issue affects DX NetOps Spectrum: 24.3.13 and earlier.	N/A	More Details
CVE-2025-14279	MLFlow versions up to and including 3.4.0 are vulnerable to DNS rebinding attacks due to a lack of Origin header validation in the MLFlow REST server. This vulnerability allows malicious websites to bypass Same-Origin Policy protections and execute unauthorized calls against REST endpoints. An attacker can query, update, and delete experiments via the affected endpoints, leading to potential data exfiltration, destruction, or manipulation. The issue is resolved in version 3.5.0.	N/A	More Details
CVE-2025-40975	Stored Cross-Site Scripting (XSS) vulnerability in WorkDo's HRMGo, consisting of a lack of proper validation of user input by sending a POST request to '/hrmgo/ticket/changereply', using the 'description' parameter.	N/A	More Details
CVE-2025-40976	Stored Cross-Site Scripting (XSS) vulnerability in WorkDo's TicketGo, consisting of a lack of proper validation of user input by sending a POST request to '/ticketgo-saas/home', using the 'description' parameter.	N/A	More Details
CVE-2025-40977	Stored Cross-Site Scripting (XSS) vulnerability in WorkDo's eCommerceGo SaaS, consisting of a lack of proper validation of user input by sending a POST request to '/store-ticket', using the 'subject' and 'description' parameters.	N/A	More Details
CVE-2026-22836	Rejected reason: Not used	N/A	More Details
CVE-2025-41004	Imaster's Patient Records Management System is vulnerable to SQL Injection in the endpoint '/projects/hospital/admin/complaints.php' through the 'id' parameter.	N/A	More Details
CVE-2026-22580	Rejected reason: Not used	N/A	More Details
CVE-2025-41005	Imaster's MEMS Events CRM contains an SQL injection vulnerability in'keyword' parameter in '/memsdemo/exchange_offers.php'.	N/A	More Details
CVE-2025-41006	Imaster's MEMS Events CRM contains an SQL injection vulnerability in 'phone' parameter in '/memsdemo/login.php'.	N/A	More Details
CVE-2025-41077	IDOR vulnerability has been found in Viafirma Inbox v4.5.13 that allows any authenticated user without privileges in the application to list all users, access and modify their data. This allows the user's email addresses to be modified and, subsequently, using the password recovery functionality to access the application by impersonating any user, including those with administrative permissions.	N/A	More Details
CVE-2025-41078	Weaknesses in the authorization mechanisms of Viafirma Documents v3.7.129 allow an authenticated user without privileges to list and access other user data, use user creation, modification, and deletion features, and escalate privileges by impersonating other users of the application in the generation and signing of documents.	N/A	More Details
CVE-2026-22581	Rejected reason: Not used	N/A	More Details
CVE-2026-22033	Label Studio is a multi-type data labeling and annotation tool. In 1.22.0 and earlier, a persistent stored cross-site scripting (XSS) vulnerability exists in the custom_hotkeys functionality of the application. An authenticated attacker (or one who can trick a user/administrator into updating their custom_hotkeys) can inject JavaScript code that executes in other users' browsers when those users load any page using the templates/base.html template. Because the application exposes an API token endpoint (/api/current-user/token) to the browser and lacks robust CSRF protection on some API endpoints, the injected script may fetch the victim's API token or call token reset endpoints — enabling full account takeover and unauthorized API access.	N/A	More Details
CVE-	ONTAP versions 9.16.1 prior to 9.16.1P9 and 9.17.1 prior to 9.17.1P2 with snapshot locking enabled are		More

2026-22050	susceptible to a vulnerability which could allow a privileged remote attacker to set the snapshot expiry time to none.	N/A	Details
CVE-2025-14470	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-22200	Enhancesoft osTicket versions up to and including 1.18.2 contain an arbitrary file read vulnerability in the ticket PDF export functionality. A remote attacker can submit a ticket containing crafted rich-text HTML that includes PHP filter expressions which are insufficiently sanitized before being processed by the mPDF PDF generator during export. When the attacker exports the ticket to PDF, the generated PDF can embed the contents of attacker-selected files from the server filesystem as bitmap images, allowing disclosure of sensitive local files in the context of the osTicket application user. This issue is exploitable in default configurations where guests may create tickets and access ticket status, or where self-registration is enabled.	N/A	More Details
CVE-2024-58339	LlamaIndex (run-llama/llama_index) versions up to and including 0.12.2 contain an uncontrolled resource consumption vulnerability in the VannaPack VannaQueryEngine implementation. The custom_query() logic generates SQL statements from a user-supplied prompt and executes them via vn.run_sql() without enforcing query execution limits In downstream deployments where untrusted users can supply prompts, an attacker can trigger expensive or unbounded SQL operations that exhaust CPU or memory resources, resulting in a denial-of-service condition. The vulnerable execution path occurs in llama_index/packs/vanna/base.py within custom_query().	N/A	More Details
CVE-2025-58411	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause mismanagement of resources reference counting creating a potential use after free scenario. Improper resource management and reference counting on an internal resource caused scenario where potential write use after free was present.	N/A	More Details
CVE-2025-58409	Software installed and run as a non-privileged user may conduct improper GPU system calls to subvert GPU HW to write to arbitrary physical memory pages. Under certain circumstances this exploit could be used to corrupt data pages not allocated by the GPU driver but memory pages in use by the kernel and drivers running on the platform altering their behaviour. This attack can lead the GPU to perform write operations on restricted internal GPU buffers that can lead to a second order affect of corrupted arbitrary physical memory.	N/A	More Details
CVE-2025-71079	In the Linux kernel, the following vulnerability has been resolved: net: nfc: fix deadlock between nfc_unregister_device and rfkill_fop_write A deadlock can occur between nfc_unregister_device() and rfkill_fop_write() due to lock ordering inversion between device_lock and rfkill_global_mutex. The problematic lock order is: Thread A (rfkill_fop_write): rfkill_fop_write() mutex_lock(&rfkill_global_mutex) rfkill_set_block() nfc_rfkill_set_block() nfc_dev_down() device_lock(&dev->dev) <- waits for device_lock Thread B (nfc_unregister_device): nfc_unregister_device() device_lock(&dev->dev) rfkill_unregister() mutex_lock(&rfkill_global_mutex) <- waits for rfkill_global_mutex This creates a classic ABBA deadlock scenario. Fix this by moving rfkill_unregister() and rfkill_destroy() outside the device_lock critical section. Store the rfkill pointer in a local variable before releasing the lock, then call rfkill_unregister() after releasing device_lock. This change is safe because rfkill_fop_write() holds rfkill_global_mutex while calling the rfkill callbacks, and rfkill_unregister() also acquires rfkill_global_mutex before cleanup. Therefore, rfkill_unregister() will wait for any ongoing callback to complete before proceeding, and device_del() is only called after rfkill_unregister() returns, preventing any use-after-free. The similar lock ordering in nfc_register_device() (device_lock -> rfkill_global_mutex via rfkill_register) is safe because during registration the device is not yet in rfkill_list, so no concurrent rfkill operations can occur on this device.	N/A	More Details
CVE-2025-71088	In the Linux kernel, the following vulnerability has been resolved: mptcp: fallback earlier on simult connection Syzkaller reports a simult-connect race leading to inconsistent fallback status: WARNING: CPU: 3 PID: 33 at net/mptcp/subflow.c:1515 subflow_data_ready+0x40b/0x7c0 net/mptcp/subflow.c:1515 Modules linked in: CPU: 3 UID: 0 PID: 33 Comm: ksoftirqd/3 Not tainted 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:subflow_data_ready+0x40b/0x7c0 net/mptcp/subflow.c:1515 Code: 89 ee e8 78 61 3c f6 40 84 ed 75 21 e8 8e 66 3c f6 44 89 fe bf 07 00 00 00 e8 c1 61 3c f6 41 83 ff 07 74 09 e8 76 66 3c f6 90 <0f> 0b 90 e8 6d 66 3c f6 48 89 df e8 e5 ad ff ff 31 ff 89 c5 89 c6 RSP: 0018:ffffc900006cf338 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff888031acd100 RCX: ffffffff8b7f2abf RDX: ffff88801e6ea440 RSI: ffffffff8b7f2aca RDI: 0000000000000005 RBP: 0000000000000000 R08: 0000000000000005 R09: 0000000000000007 R10: 0000000000000004 R11: 0000000000002c10 R12: ffff88802ba69900 R13: 1ffff920000d9e67 R14: ffff888046f81800 R15: 0000000000000004 FS: 0000000000000000(0000) GS:ffff8880d69bc000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000560fc0ca1670 CR3: 0000000032c3a000 CR4: 0000000000352ef0 Call Trace: <TASK> tcp_data_queue+0x13b0/0x4f90 net/ipv4/tcp_input.c:5197 tcp_rcv_state_process+0xfdf/0x4ec0 net/ipv4/tcp_input.c:6922 tcp_v6_do_rcv+0x492/0x1740 net/ipv6/tcp_ipv6.c:1672 tcp_v6_rcv+0x2976/0x41e0 net/ipv6/tcp_ipv6.c:1918 ip6_protocol_deliver_rcu+0x188/0x1520 net/ipv6/ip6_input.c:438 ip6_input_finish+0x1e4/0x4b0 net/ipv6/ip6_input.c:489 NF_HOOK include/linux/netfilter.h:318 [inline] NF_HOOK include/linux/netfilter.h:312 [inline] ip6_input+0x105/0x2f0 net/ipv6/ip6_input.c:500 dst_input include/net/dst.h:471 [inline] ip6_rcv_finish net/ipv6/ip6_input.c:79 [inline] NF_HOOK include/linux/netfilter.h:318 [inline] NF_HOOK	N/A	More Details

	include/linux/netfilter.h:312 [inline] ipv6_rcv+0x264/0x650 net/ipv6/ip6_input.c:311 __netif_receive_skb_one_core+0x12d/0x1e0 net/core/dev.c:5979 __netif_receive_skb+0x1d/0x160 net/core/dev.c:6092 process_backlog+0x442/0x15e0 net/core/dev.c:6444 __napi_poll.constprop.0+0xba/0x550 net/core/dev.c:7494 napi_poll net/core/dev.c:7557 [inline] net_rx_action+0xa9f/0xfe0 net/core/dev.c:7684 handle_softirqs+0x216/0x8e0 kernel/softirq.c:579 run_ksoftirqd kernel/softirq.c:968 [inline] run_ksoftirqd+0x3a/0x60 kernel/softirq.c:960 smpboot_thread_fn+0x3f7/0xae0 kernel/smpboot.c:160 kthread+0x3c2/0x780 kernel/kthread.c:463 ret_from_fork+0x5d7/0x6f0 arch/x86/kernel/process.c:148 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> The TCP subflow can process the simult-connect syn-ack packet after transitioning to TCP_FIN1 state, bypassing the MPTCP fallback check, as the sk_state_change() callback is not invoked for * -> FIN_WAIT1 transitions. That will move the msk socket to an inconsistent status and the next incoming data will hit the reported splat. Close the race moving the simult-fallback check at the earliest possible stage - that is at syn-ack generation time. About the fixes tags: [2] was supposed to also fix this issue introduced by [3]. [1] is required as a dependence: it was not explicitly marked as a fix, but it is one and it has already been backported before [3]. In other words, this commit should be backported up to [3], including [2] and [1] if that's not already there.		
CVE-2025-71087	In the Linux kernel, the following vulnerability has been resolved: iavf: fix off-by-one issues in iavf_config_rss_reg() There are off-by-one bugs when configuring RSS hash key and lookup table, causing out-of-bounds reads to memory [1] and out-of-bounds writes to device registers. Before commit 43a3d9ba34c9 ("i40evf: Allow PF driver to configure RSS"), the loop upper bounds were: i <= I40E_VFQF_{HKEY,HLUT}_MAX_INDEX which is safe since the value is the last valid index. That commit changed the bounds to: i <= adapter->rss_{key,lut}_size / 4 where `rss_{key,lut}_size / 4` is the number of dwords, so the last valid index is `(rss_{key,lut}_size / 4) - 1`. Therefore, using `<=` accesses one element past the end. Fix the issues by using `<` instead of `<=`, ensuring we do not exceed the bounds. [1] KASAN splat about rss_key_size off-by-one BUG: KASAN: slab-out-of-bounds in iavf_config_rss+0x619/0x800 Read of size 4 at addr ffff888102c50134 by task kworker/u8:6/63 CPU: 0 UID: 0 PID: 63 Comm: kworker/u8:6 Not tainted 6.18.0-rc2-enjuk-tnguy-00378-g3005f5b77652-dirty #156 PREEMPT(voluntary) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Workqueue: iavf iavf_watchdog_task Call Trace: <TASK> dump_stack_lvl+0x6f/0xb0 print_report+0x170/0x4f3 kasan_report+0xe1/0x1a0 iavf_config_rss+0x619/0x800 iavf_watchdog_task+0x2be7/0x3230 process_one_work+0x7fd/0x1420 worker_thread+0x4d1/0xd40 kthread+0x344/0x660 ret_from_fork+0x249/0x320 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 63: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x7f/0x90 __kmalloc_noprof+0x246/0x6f0 iavf_watchdog_task+0x28fc/0x3230 process_one_work+0x7fd/0x1420 worker_thread+0x4d1/0xd40 kthread+0x344/0x660 ret_from_fork+0x249/0x320 ret_from_fork_asm+0x1a/0x30 The buggy address belongs to the object at ffff888102c50100 which belongs to the cache kmalloc-64 of size 64 The buggy address is located 0 bytes to the right of allocated 52-byte region [ffff888102c50100, ffff888102c50134) The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x102c50 flags: 0x200000000000000(node=0|zone=2) page_type: f5(slab) raw: 0200000000000000 ffff8881000418c0 dead000000000122 0000000000000000 raw: 0000000000000000 0000000080200020 00000000f5000000 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff888102c50000: 00 00 00 00 00 00 00 fc fc fc fc fc fc fc fc fc ffff888102c50080: 00 00 00 00 00 00 00 fc fc fc fc fc fc fc fc fc >ffff888102c50100: 00 00 00 00 00 00 04 fc fc fc fc fc fc fc fc fc ^ ffff888102c50180: 00 00 00 00 00 00 00 fc fc fc fc fc fc fc fc fc ffff888102c50200: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc	N/A	More Details
CVE-2025-71086	In the Linux kernel, the following vulnerability has been resolved: net: rose: fix invalid array index in rose_kill_by_device() rose_kill_by_device() collects sockets into a local array[] and then iterates over them to disconnect sockets bound to a device being brought down. The loop mistakenly indexes array[cnt] instead of array[i]. For cnt < ARRAY_SIZE(array), this reads an uninitialized entry; for cnt == ARRAY_SIZE(array), it is an out-of-bounds read. Either case can lead to an invalid socket pointer dereference and also leaks references taken via sock_hold(). Fix the index to use i.	N/A	More Details
CVE-2025-71085	In the Linux kernel, the following vulnerability has been resolved: ipv6: BUG() in pskb_expand_head() as part of calipso_skbuff_setattr() There exists a kernel oops caused by a BUG_ON(nhead < 0) at net/core/skbuff.c:2232 in pskb_expand_head(). This bug is triggered as part of the calipso_skbuff_setattr() routine when skb_cow() is passed headroom > INT_MAX (i.e. (int)(skb_headroom(skb) + len_delta) < 0). The root cause of the bug is due to an implicit integer cast in __skb_cow(). The check (headroom > skb_headroom(skb)) is meant to ensure that delta = headroom - skb_headroom(skb) is never negative, otherwise we will trigger a BUG_ON in pskb_expand_head(). However, if headroom > INT_MAX and delta <= -NET_SKB_PAD, the check passes, delta becomes negative, and pskb_expand_head() is passed a negative value for nhead. Fix the trigger condition in calipso_skbuff_setattr(). Avoid passing "negative" headroom sizes to skb_cow() within calipso_skbuff_setattr() by only using skb_cow() to grow headroom. PoC: Using `netlabelctl` tool: netlabelctl map del default netlabelctl calipso add pass doi:7 netlabelctl map add default address:0::1/128 protocol:calipso,7 Then run the following PoC: int fd = socket(AF_INET6, SOCK_DGRAM, IPPROTO_UDP); // setup msghdr int cmsg_size = 2; int cmsg_len = 0x60; struct msghdr msg; struct sockaddr_in6 dest_addr; struct cmsghdr * cmsg = (struct cmsghdr *) calloc(1, sizeof(struct cmsghdr) + cmsg_len); msg.msg_name = &dest_addr; msg.msg_namelen = sizeof(dest_addr); msg.msg_iov = NULL;	N/A	More Details

	msg.msg_iovlen = 0; msg.msg_control = cmsg; msg.msg_controllen = cmsg_len; msg.msg_flags = 0; // setup sockaddr dest_addr.sin6_family = AF_INET6; dest_addr.sin6_port = htons(31337); dest_addr.sin6_flowinfo = htonl(31337); dest_addr.sin6_addr = in6addr_loopback; dest_addr.sin6_scope_id = 31337; // setup cmsghdr cmsg->cmsg_len = cmsg_len; cmsg->cmsg_level = IPPROTO_IPV6; cmsg->cmsg_type = IPV6_HOPOPTS; char * hop_hdr = (char *)cmsg + sizeof(struct cmsghdr); hop_hdr[1] = 0x9; //set hop size - (0x9 + 1) * 8 = 80 sendmsg(fd, &msg, 0);		
CVE-2025-71084	In the Linux kernel, the following vulnerability has been resolved: RDMA/cm: Fix leaking the multicast GID table reference If the CM ID is destroyed while the CM event for multicast creating is still queued the cancel_work_sync() will prevent the work from running which also prevents destroying the ah_attr. This leaks a refcount and triggers a WARN: GID entry ref leak for dev syz1 index 2 ref=573 WARNING: CPU: 1 PID: 655 at drivers/infiniband/core/cache.c:809 release_gid_table drivers/infiniband/core/cache.c:806 [inline] WARNING: CPU: 1 PID: 655 at drivers/infiniband/core/cache.c:809 gid_table_release_one+0x284/0x3cc drivers/infiniband/core/cache.c:886 Destroy the ah_attr after canceling the work, it is safe to call this twice.	N/A	More Details
CVE-2025-71083	In the Linux kernel, the following vulnerability has been resolved: drm/ttm: Avoid NULL pointer deref for evicted BOs It is possible for a BO to exist that is not currently associated with a resource, e.g. because it has been evicted. When devcoredump tries to read the contents of all BOs for dumping, we need to expect this as well -- in this case, ENODATA is recorded instead of the buffer contents.	N/A	More Details
CVE-2025-71082	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: revert use of devm_kzalloc in btusb This reverts commit 98921dbd00c4e ("Bluetooth: Use devm_kzalloc in btusb.c file"). In btusb_probe(), we use devm_kzalloc() to allocate the btusb data. This ties the lifetime of all the btusb data to the binding of a driver to one interface, INTF. In a driver that binds to other interfaces, ISOC and DIAG, this is an accident waiting to happen. The issue is revealed in btusb_disconnect(), where calling usb_driver_release_interface(&btusb_driver, data->intf) will have devm free the data that is also being used by the other interfaces of the driver that may not be released yet. To fix this, revert the use of devm and go back to freeing memory explicitly.	N/A	More Details
CVE-2025-71081	In the Linux kernel, the following vulnerability has been resolved: ASoC: stm32: sai: fix OF node leak on probe The reference taken to the sync provider OF node when probing the platform device is currently only dropped if the set_sync() callback fails during DAI probe. Make sure to drop the reference on platform probe failures (e.g. probe deferral) and on driver unbind. This also avoids a potential use-after-free in case the DAI is ever reprobed without first rebinding the platform driver.	N/A	More Details
CVE-2025-71080	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix a BUG in rt6_get_pcpu_route() under PREEMPT_RT On PREEMPT_RT kernels, after rt6_get_pcpu_route() returns NULL, the current task can be preempted. Another task running on the same CPU may then execute rt6_make_pcpu_route() and successfully install a pcpu_rt entry. When the first task resumes execution, its cmpxchg() in rt6_make_pcpu_route() will fail because rt6i_pcpu is no longer NULL, triggering the BUG_ON(prev). It's easy to reproduce it by adding mdelay() after rt6_get_pcpu_route(). Using preempt_disable/enable is not appropriate here because ip6_rt_pcpu_alloc() may sleep. Fix this by handling the cmpxchg() failure gracefully on PREEMPT_RT: free our allocation and return the existing pcpu_rt installed by another task. The BUG_ON is replaced by WARN_ON_ONCE for non-PREEMPT_RT kernels where such races should not occur.	N/A	More Details
CVE-2025-71078	In the Linux kernel, the following vulnerability has been resolved: powerpc/64s/slb: Fix SLB multihit issue during SLB preload On systems using the hash MMU, there is a software SLB preload cache that mirrors the entries loaded into the hardware SLB buffer. This preload cache is subject to periodic eviction — typically after every 256 context switches — to remove old entry. To optimize performance, the kernel skips switch_mmu_context() in switch_mm_irqs_off() when the prev and next mm_struct are the same. However, on hash MMU systems, this can lead to inconsistencies between the hardware SLB and the software preload cache. If an SLB entry for a process is evicted from the software cache on one CPU, and the same process later runs on another CPU without executing switch_mmu_context(), the hardware SLB may retain stale entries. If the kernel then attempts to reload that entry, it can trigger an SLB multi-hit error. The following timeline shows how stale SLB entries are created and can cause a multi-hit error when a process moves between CPUs without a MMU context switch. CPU 0 CPU 1 ----- ----- Process P exec swapper/1 load_elf_binary begin_new_exc activate_mm switch_mm_irqs_off switch_mmu_context switch_slb /* * This invalidates all * the entries in the HW * and setup the new HW * SLB entries as per the * preload cache. */ context_switch sched_migrate_task migrates process P to cpu-1 Process swapper/0 context switch (to process P) (uses mm_struct of Process P) switch_mm_irqs_off() switch_slb load_slb++ /* * load_slb becomes 0 here * and we evict an entry from * the preload cache with * preload_age(). We still * keep HW SLB and preload * cache in sync, that is * because all HW SLB entries * anyways gets evicted in * switch_slb during SLBIA. * We then only add those * entries back in HW SLB, * which are currently * present in preload_cache * (after eviction). */ load_elf_binary continues... setup_new_exec() slb_setup_new_exec() sched_switch event sched_migrate_task migrates process P to cpu-0 context_switch from swapper/0 to Process P switch_mm_irqs_off() /* * Since both prev and next mm struct are same we don't call * switch_mmu_context(). This will cause the HW SLB and SW preload * cache to go out of sync in preload_new_slb_context. Because there * was an SLB entry which was evicted from both HW and preload cache * on cpu-1. Now later in preload_new_slb_context(), when we will try * to add the same preload entry again, we will add this to the SW * preload cache and then will add it to the HW SLB. Since on cpu-0 * this entry was never invalidated, hence adding this entry to the HW * SLB will cause a SLB multi-hit error. */ load_elf_binary cont ---truncated---	N/A	More Details

CVE-2024-58340	LangChain versions up to and including 0.3.1 contain a regular expression denial-of-service (ReDoS) vulnerability in the MRKLOutputParser.parse() method (libs/langchain/langchain/agents/mrkl/output_parser.py). The parser applies a backtracking-prone regular expression when extracting tool actions from model output. An attacker who can supply or influence the parsed text (for example via prompt injection in downstream applications that pass LLM output directly into MRKLOutputParser.parse()) can trigger excessive CPU consumption by providing a crafted payload, causing significant parsing delays and a denial-of-service condition.	N/A	More Details
CVE-2025-71077	In the Linux kernel, the following vulnerability has been resolved: tpm: Cap the number of PCR banks tpm2_get_pcr_allocation() does not cap any upper limit for the number of banks. Cap the limit to eight banks so that out of bounds values coming from external I/O cause on only limited harm.	N/A	More Details
CVE-2025-71076	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Limit num_syncs to prevent oversized allocations The OA open parameters did not validate num_syncs, allowing userspace to pass arbitrarily large values, potentially leading to excessive allocations. Add check to ensure that num_syncs does not exceed DRM_XE_MAX_SYNCS, returning -EINVAL when the limit is violated. v2: use XE_IOCTL_DBG() and drop duplicated check. (Ashutosh) (cherry picked from commit e057b2d2b8d815df3858a87dffafa2af37e5945b)	N/A	More Details
CVE-2025-71075	In the Linux kernel, the following vulnerability has been resolved: scsi: aic94xx: fix use-after-free in device removal path The asd_pci_remove() function fails to synchronize with pending tasklets before freeing the asd_ha structure, leading to a potential use-after-free vulnerability. When a device removal is triggered (via hot-unplug or module unload), race condition can occur. The fix adds tasklet_kill() before freeing the asd_ha structure, ensuring all scheduled tasklets complete before cleanup proceeds.	N/A	More Details
CVE-2025-71074	In the Linux kernel, the following vulnerability has been resolved: functionfs: fix the open/removal races ffs_epfile_open() can race with removal, ending up with file->private_data pointing to freed object. There is a total count of opened files on functionfs (both ep0 and dynamic ones) and when it hits zero, dynamic files get removed. Unfortunately, that removal can happen while another thread is in ffs_epfile_open(), but has not incremented the count yet. In that case open will succeed, leaving us with UAF on any subsequent read() or write(). The root cause is that ffs->opened is misused; atomic_dec_and_test() vs. atomic_add_return() is not a good idea, when object remains visible all along. To untangle that * serialize openers on ffs->mutex (both for ep0 and for dynamic files) * have dynamic ones use atomic_inc_not_zero() and fail if we had zero ->opened; in that case the file we are opening is doomed. * have the inodes of dynamic files marked on removal (from the callback of simple_recursive_removal()) - clear ->i_private there. * have open of dynamic ones verify they hadn't been already removed, along with checking that state is FFS_ACTIVE.	N/A	More Details
CVE-2025-71073	In the Linux kernel, the following vulnerability has been resolved: Input: lkkbd - disable pending work before freeing device lkkbd_interrupt() schedules lk->tq via schedule_work(), and the work handler lkkbd_reinit() dereferences the lkkbd structure and its serio/input_dev fields. lkkbd_disconnect() and error paths in lkkbd_connect() free the lkkbd structure without preventing the reinit work from being queued again until serio_close() returns. This can allow the work handler to run after the structure has been freed, leading to a potential use-after-free. Use disable_work_sync() instead of cancel_work_sync() to ensure the reinit work cannot be re-queued, and call it both in lkkbd_disconnect() and in lkkbd_connect() error paths after serio_open().	N/A	More Details
CVE-2025-71072	In the Linux kernel, the following vulnerability has been resolved: shmem: fix recovery on rename failures maple_tree insertions can fail if we are seriously short on memory; simple_offset_rename() does not recover well if it runs into that. The same goes for simple_offset_rename_exchange(). Moreover, shmem_whiteout() expects that if it succeeds, the caller will progress to d_move(), i.e. that shmem_rename2() won't fail past the successful call of shmem_whiteout(). Not hard to fix, fortunately - mtree_store() can't fail if the index we are trying to store into is already present in the tree as a singleton. For simple_offset_rename_exchange() that's enough - we just need to be careful about the order of operations. For simple_offset_rename() solution is to preinsert the target into the tree for new_dir; the rest can be done without any potentially failing operations. That preinsertion has to be done in shmem_rename2() rather than in simple_offset_rename() itself - otherwise we'd need to deal with the possibility of failure after successful shmem_whiteout().	N/A	More Details
CVE-2025-71071	In the Linux kernel, the following vulnerability has been resolved: iommu/mediatek: fix use-after-free on probe deferral The driver is dropping the references taken to the larb devices during probe after successful lookup as well as on errors. This can potentially lead to a use-after-free in case a larb device has not yet been bound to its driver so that the iommu driver probe defers. Fix this by keeping the references as expected while the iommu driver is bound.	N/A	More Details
CVE-2025-71070	In the Linux kernel, the following vulnerability has been resolved: ublk: clean up user copy references on ublk server exit If a ublk server process releases a ublk char device file, any requests dispatched to the ublk server but not yet completed will retain a ref value of UBLK_REFCOUNT_INIT. Before commit e63d2228ef83 ("ublk: simplify aborting ublk request"), __ublk_fail_req() would decrement the reference count before completing the failed request. However, that commit optimized __ublk_fail_req() to call __ublk_complete_rq() directly without decrementing the request reference count. The leaked reference count incorrectly allows user copy and zero copy operations on the completed ublk request. It also triggers the WARN_ON_ONCE(refcount_read(&io->ref)) warnings in ublk_queue_reinit() and ublk_deinit_queue(). Commit	N/A	More Details

	c5c5eb24ed61 ("ublk: avoid ublk_io_release() called after ublk char dev is closed") already fixed the issue for ublk devices using UBLK_F_SUPPORT_ZERO_COPY or UBLK_F_AUTO_BUF_REG. However, the reference count leak also affects UBLK_F_USER_COPY, the other reference-counted data copy mode. Fix the condition in ublk_check_and_reset_active_ref() to include all reference-counted data copy modes. This ensures that any ublk requests still owned by the ublk server when it exits have their reference counts reset to 0.		
CVE-2025-71069	In the Linux kernel, the following vulnerability has been resolved: f2fs: invalidate dentry cache on failed whiteout creation F2FS can mount filesystems with corrupted directory depth values that get runtime-clamped to MAX_DIR_HASH_DEPTH. When RENAME_WHITEOUT operations are performed on such directories, f2fs_rename performs directory modifications (updating target entry and deleting source entry) before attempting to add the whiteout entry via f2fs_add_link. If f2fs_add_link fails due to the corrupted directory structure, the function returns an error to VFS, but the partial directory modifications have already been committed to disk. VFS assumes the entire rename operation failed and does not update the dentry cache, leaving stale mappings. In the error path, VFS does not call d_move() to update the dentry cache. This results in new_dentry still pointing to the old inode (new_inode) which has already had its i_nlink decremented to zero. The stale cache causes subsequent operations to incorrectly reference the freed inode. This causes subsequent operations to use cached dentry information that no longer matches the on-disk state. When a second rename targets the same entry, VFS attempts to decrement i_nlink on the stale inode, which may already have i_nlink=0, triggering a WARNING in drop_nlink(). Example sequence: 1. First rename (RENAME_WHITEOUT): file2 → file1 - f2fs updates file1 entry on disk (points to inode 8) - f2fs deletes file2 entry on disk - f2fs_add_link(whiteout) fails (corrupted directory) - Returns error to VFS - VFS does not call d_move() due to error - VFS cache still has: file1 → inode 7 (stale!) - inode 7 has i_nlink=0 (already decremented) 2. Second rename: file3 → file1 - VFS uses stale cache: file1 → inode 7 - Tries to drop_nlink on inode 7 (i_nlink already 0) - WARNING in drop_nlink() Fix this by explicitly invalidating old_dentry and new_dentry when f2fs_add_link fails during whiteout creation. This forces VFS to refresh from disk on subsequent operations, ensuring cache consistency even when the rename partially succeeds. Reproducer: 1. Mount F2FS image with corrupted i_current_depth 2. renameat2(file2, file1, RENAME_WHITEOUT) 3. renameat2(file3, file1, 0) 4. System triggers WARNING in drop_nlink()	N/A	More Details
CVE-2025-71089	In the Linux kernel, the following vulnerability has been resolved: iommu: disable SVA when CONFIG_X86 is set Patch series "Fix stale IOTLB entries for kernel address space", v7. This proposes a fix for a security vulnerability related to IOMMU Shared Virtual Addressing (SVA). In an SVA context, an IOMMU can cache kernel page table entries. When a kernel page table page is freed and reallocated for another purpose, the IOMMU might still hold stale, incorrect entries. This can be exploited to cause a use-after-free or write-after-free condition, potentially leading to privilege escalation or data corruption. This solution introduces a deferred freeing mechanism for kernel page table pages, which provides a safe window to notify the IOMMU to invalidate its caches before the page is reused. This patch (of 8): In the IOMMU Shared Virtual Addressing (SVA) context, the IOMMU hardware shares and walks the CPU's page tables. The x86 architecture maps the kernel's virtual address space into the upper portion of every process's page table. Consequently, in an SVA context, the IOMMU hardware can walk and cache kernel page table entries. The Linux kernel currently lacks a notification mechanism for kernel page table changes, specifically when page table pages are freed and reused. The IOMMU driver is only notified of changes to user virtual address mappings. This can cause the IOMMU's internal caches to retain stale entries for kernel VA. Use-After-Free (UAF) and Write-After-Free (WAF) conditions arise when kernel page table pages are freed and later reallocated. The IOMMU could misinterpret the new data as valid page table entries. The IOMMU might then walk into attacker-controlled memory, leading to arbitrary physical memory DMA access or privilege escalation. This is also a Write-After-Free issue, as the IOMMU will potentially continue to write Accessed and Dirty bits to the freed memory while attempting to walk the stale page tables. Currently, SVA contexts are unprivileged and cannot access kernel mappings. However, the IOMMU will still walk kernel-only page tables all the way down to the leaf entries, where it realizes the mapping is for the kernel and errors out. This means the IOMMU still caches these intermediate page table entries, making the described vulnerability a real concern. Disable SVA on x86 architecture until the IOMMU can receive notification to flush the paging cache before freeing the CPU kernel page table pages.	N/A	More Details
CVE-2025-71090	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfsd_file reference leak in nfsd4_add_rdaccess_to_wrdeleg() nfsd4_add_rdaccess_to_wrdeleg() unconditionally overwrites fp->fi_fds[O_RDONLY] with a newly acquired nfsd_file. However, if the client already has a SHARE_ACCESS_READ open from a previous OPEN operation, this action overwrites the existing pointer without releasing its reference, orphaning the previous reference. Additionally, the function originally stored the same nfsd_file pointer in both fp->fi_fds[O_RDONLY] and fp->fi_rdeleg_file with only a single reference. When put_deleg_file() runs, it clears fi_rdeleg_file and calls nfs4_file_put_access() to release the file. However, nfs4_file_put_access() only releases fi_fds[O_RDONLY] when the fi_access[O_RDONLY] counter drops to zero. If another READ open exists on the file, the counter remains elevated and the nfsd_file reference from the delegation is never released. This potentially causes open conflicts on that file. Then, on server shutdown, these leaks cause __nfsd_file_cache_purge() to encounter files with an elevated reference count that cannot be cleaned up, ultimately triggering a BUG() in kmem_cache_destroy() because there are still nfsd_file objects allocated in that cache.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: team: fix check for port enabled in team_queue_override_port_prio_changed() There has been a syzkaller bug reported recently with the following trace: list_del corruption, ffff888058bea080->prev is LIST_POISON2 (dead000000000122) ----------[		

CVE-2025-71091	cut here]---------- kernel BUG at lib/list_debug.c:59! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 3 UID: 0 PID: 21246 Comm: syz.0.2928 Not tainted 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:__list_del_entry_valid_or_report+0x13e/0x200 lib/list_debug.c:59 Code: 48 c7 c7 e0 71 f0 8b e8 30 08 ef fc 90 0f 0b 48 89 ef e8 a5 02 55 fd 48 89 ea 48 89 de 48 c7 c7 40 72 f0 8b e8 13 08 ef fc 90 <0f> 0b 48 89 ef e8 88 02 55 fd 48 89 ea 48 b8 00 00 00 00 00 fc ff RSP: 0018:ffffc9000d49f370 EFLAGS: 00010286 RAX: 000000000000004e RBX: ffff888058bea080 RCX: ffffc9002817d000 RDX: 0000000000000000 RSI: ffffffff819becc6 RDI: 0000000000000005 RBP: dead000000000122 R08: 0000000000000005 R09: 0000000000000000 R10: 0000000080000000 R11: 0000000000000001 R12: ffff888039e9c230 R13: ffff888058bea088 R14: ffff888058bea080 R15: ffff888055461480 FS: 00007fbbcfe6f6c0(0000) GS:ffff8880d6d0a000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000110c3afcb0 CR3: 00000000382c7000 CR4: 0000000000352ef0 Call Trace: <TASK> __list_del_entry_valid include/linux/list.h:132 [inline] __list_del_entry include/linux/list.h:223 [inline] list_del_rcu include/linux/rculist.h:178 [inline] __team_queue_override_port_del drivers/net/team/team_core.c:826 [inline] __team_queue_override_port_del drivers/net/team/team_core.c:821 [inline] team_queue_override_port_prio_changed drivers/net/team/team_core.c:883 [inline] team_priority_option_set+0x171/0x2f0 drivers/net/team/team_core.c:1534 team_option_set drivers/net/team/team_core.c:376 [inline] team_nl_options_set_doit+0x8ae/0xe60 drivers/net/team/team_core.c:2653 genl_family_rcv_msg_doit+0x209/0x2f0 net/netlink/genetlink.c:1115 genl_family_rcv_msg net/netlink/genetlink.c:1195 [inline] genl_rcv_msg+0x55c/0x800 net/netlink/genetlink.c:1210 netlink_rcv_skb+0x158/0x420 net/netlink/af_netlink.c:2552 genl_rcv+0x28/0x40 net/netlink/genetlink.c:1219 netlink_unicast_kernel net/netlink/af_netlink.c:1320 [inline] netlink_unicast+0x5aa/0x870 net/netlink/af_netlink.c:1346 netlink_sendmsg+0x8c8/0xdd0 net/netlink/af_netlink.c:1896 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa98/0xc70 net/socket.c:2630 ___sys_sendmsg+0x134/0x1d0 net/socket.c:2684 __sys_sendmsg+0x16d/0x220 net/socket.c:2716 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xcd/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f The problem is in this flow: 1) Port is enabled, queue_id != 0, in qom_list 2) Port gets disabled -> team_port_disable() -> team_queue_override_port_del() -> del (removed from list) 3) Port is disabled, queue_id != 0, not in any list 4) Priority changes -> team_queue_override_port_prio_changed() -> checks: port disabled && queue_id != 0 -> calls del - hits the BUG as it is removed already To fix this, change the check in team_queue_override_port_prio_changed() so it returns early if port is not enabled.	N/A	More Details
CVE-2025-71092	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Fix OOB write in bnxt_re_copy_err_stats() Commit ef56081d1864 ("RDMA/bnxt_re: RoCE related hardware counters update") added three new counters and placed them after BNXT_RE_OUT_OF_SEQ_ERR. BNXT_RE_OUT_OF_SEQ_ERR acts as a boundary marker for allocating hardware statistics with different num_counters values on chip_gen_p5_p7 devices. As a result, BNXT_RE_NUM_STD_COUNTERS are used when allocating hw_stats, which leads to an out-of-bounds write in bnxt_re_copy_err_stats(). The counters BNXT_RE_REQ_CQE_ERROR, BNXT_RE_RESP_CQE_ERROR, and BNXT_RE_RESP_REMOTE_ACCESS_ERRS are applicable to generic hardware, not only p5/p7 devices. Fix this by moving these counters before BNXT_RE_OUT_OF_SEQ_ERR so they are included in the generic counter set.	N/A	More Details
CVE-2025-15514	Ollama 0.11.5-rc0 through current version 0.13.5 contain a null pointer dereference vulnerability in the multi-modal model image processing functionality. When processing base64-encoded image data via the /api/chat endpoint, the application fails to validate that the decoded data represents valid media before passing it to the mtmd_helper_bitmap_init_from_buf function. This function can return NULL for malformed input, but the code does not check this return value before dereferencing the pointer in subsequent operations. A remote attacker can exploit this by sending specially crafted base64 image data that decodes to invalid media, causing a segmentation fault and crashing the runner process. This results in a denial of service condition where the model becomes unavailable to all users until the service is restarted.	N/A	More Details
CVE-2025-25652	In Eptura Archibus 2024.03.01.109, the "Run script" and "Server File" components of the "Database Update Wizard" are vulnerable to directory traversal.	N/A	More Details
CVE-2026-22212	TinyOS versions up to and including 2.1.2 contain a stack-based buffer overflow vulnerability in the mcp2200gpio utility. The vulnerability is caused by unsafe use of strcpy() and strcat() functions when constructing device paths during automatic device discovery. A local attacker can exploit this by creating specially crafted filenames under /dev/usb/, leading to stack memory corruption and application crashes.	N/A	More Details
CVE-2025-25176	Intermediate register values of secure workloads can be exfiltrated in workloads scheduled from applications running in the non-secure environment of a platform.	N/A	More Details
CVE-2026-0408	A path traversal vulnerability in NETGEAR WiFi range extenders allows an attacker with LAN authentication to access the router's IP and review the contents of the dynamically generated webproc file, which records the username and password submitted to the router GUI.	N/A	More Details
CVE-2026-	An insufficient authentication vulnerability in NETGEAR WiFi range extenders allows a network adjacent attacker with WiFi authentication or a physical Ethernet port connection to bypass the authentication process	N/A	More Details

0407	and access the admin panel.		
CVE-2026-0406	An insufficient input validation vulnerability in the NETGEAR XR1000v2 allows attackers connected to the router's LAN to execute OS command injections.	N/A	More Details
CVE-2026-0405	An authentication bypass vulnerability in NETGEAR Orbi devices allows users connected to the local network to access the router web interface as an admin.	N/A	More Details
CVE-2026-0404	An insufficient input validation vulnerability in NETGEAR Orbi devices' DHCPv6 functionality allows network adjacent attackers authenticated over WiFi or on LAN to execute OS command injections on the router. DHCPv6 is not enabled by default.	N/A	More Details
CVE-2026-0403	An insufficient input validation vulnerability in NETGEAR Orbi routers allows attackers connected to the router's LAN to execute OS command injections.	N/A	More Details
CVE-2025-71101	In the Linux kernel, the following vulnerability has been resolved: platform/x86: hp-bioscfg: Fix out-of-bounds array access in ACPI package parsing The hp_populate_*_elements_from_package() functions in the hp-bioscfg driver contain out-of-bounds array access vulnerabilities. These functions parse ACPI packages into internal data structures using a for loop with index variable 'elem' that iterates through enum_obj/integer_obj/order_obj/password_obj/string_obj arrays. When processing multi-element fields like PREREQUISITES and ENUM_POSSIBLE_VALUES, these functions read multiple consecutive array elements using expressions like 'enum_obj[elem + reqs]' and 'enum_obj[elem + pos_values]' within nested loops. The bug is that the bounds check only validated elem, but did not consider the additional offset when accessing elem + reqs or elem + pos_values. The fix changes the bounds check to validate the actual accessed index.	N/A	More Details
CVE-2025-71100	In the Linux kernel, the following vulnerability has been resolved: wifi: rtlwifi: 8192cu: fix tid out of range in rtl92cu_tx_fill_desc() TID getting from ieee80211_get_tid() might be out of range of array size of sta_entry->tids[], so check TID is less than MAX_TID_COUNT. Othwerwise, UBSAN warn: UBSAN: array-index-out-of-bounds in drivers/net/wireless/realtek/rtlwifi/rtl8192cu/trx.c:514:30 index 10 is out of range for type 'rtl_tid_data [9]'	N/A	More Details
CVE-2025-71099	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Fix potential UAF in xe_oa_add_config_ioctl() In xe_oa_add_config_ioctl(), we accessed oa_config->id after dropping metrics_lock. Since this lock protects the lifetime of oa_config, an attacker could guess the id and call xe_oa_remove_config_ioctl() with perfect timing, freeing oa_config before we dereference it, leading to a potential use-after-free. Fix this by caching the id in a local variable while holding the lock. v2: (Matt A) - Dropped mutex_unlock(&oa->metrics_lock) ordering change from xe_oa_remove_config_ioctl() (cherry picked from commit 28aeaed130e8e587fd1b73b6d66ca41ccc5a1a31)	N/A	More Details
CVE-2025-71098	In the Linux kernel, the following vulnerability has been resolved: ip6_gre: make ip6gre_header() robust Over the years, syzbot found many ways to crash the kernel in ip6gre_header() [1]. This involves team or bonding drivers ability to dynamically change their dev->needed_headroom and/or dev->hard_header_len In this particular crash mld_newpack() allocated an skb with a too small reserve/headroom, and by the time mld_sendpack() was called, syzbot managed to attach an ip6gre device. [1] skbuff: skb_under_panic: text:ffffffff8a1d69a8 len:136 put:40 head:ffff888059bc7000 data:ffff888059bc6fe8 tail:0x70 end:0x6c0 dev:team0 ------------[cut here]------------ kernel BUG at net/core/skbuff.c:213 ! <TASK> skb_under_panic net/core/skbuff.c:223 [inline] skb_push+0xc3/0xe0 net/core/skbuff.c:2641 ip6gre_header+0xc8/0x790 net/ipv6/ip6_gre.c:1371 dev_hard_header include/linux/netdevice.h:3436 [inline] neigh_connected_output+0x286/0x460 net/core/neighbour.c:1618 neigh_output include/net/neighbour.h:556 [inline] ip6_finish_output2+0xfb3/0x1480 net/ipv6/ip6_output.c:136 __ip6_finish_output net/ipv6/ip6_output.c:-1 [inline] ip6_finish_output+0x234/0x7d0 net/ipv6/ip6_output.c:220 NF_HOOK_COND include/linux/netfilter.h:307 [inline] ip6_output+0x340/0x550 net/ipv6/ip6_output.c:247 NF_HOOK+0x9e/0x380 include/linux/netfilter.h:318 mld_sendpack+0x8d4/0xe60 net/ipv6/mcast.c:1855 mld_send_cr net/ipv6/mcast.c:2154 [inline] mld_ifc_work+0x83e/0xd60 net/ipv6/mcast.c:2693	N/A	More Details
CVE-2025-71097	In the Linux kernel, the following vulnerability has been resolved: ipv4: Fix reference count leak when using error routes with nexthop objects When a nexthop object is deleted, it is marked as dead and then fib_table_flush() is called to flush all the routes that are using the dead nexthop. The current logic in fib_table_flush() is to only flush error routes (e.g., blackhole) when it is called as part of network namespace dismantle (i.e., with flush_all=true). Therefore, error routes are not flushed when their nexthop object is deleted: # ip link add name dummy1 up type dummy # ip nexthop add id 1 dev dummy1 # ip route add 198.51.100.1/32 nhid 1 # ip route add blackhole 198.51.100.2/32 nhid 1 # ip nexthop del id 1 # ip route show blackhole 198.51.100.2 nhid 1 dev dummy1 As such, they keep holding a reference on the nexthop object which in turn holds a reference on the nexthop device, resulting in a reference count leak: # ip link del dev dummy1 [70.516258] unregister_netdevice: waiting for dummy1 to become free. Usage count = 2 Fix by flushing error routes when their nexthop is marked as dead. IPv6 does not suffer from this problem.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Check for the presence of LS_NLA_TYPE_DGID correctly The netlink response for RDMA_NL_LS_OP_IP_RESOLVE should always have a		

CVE-2025-71096	LS_NLA_TYPE_DGID attribute, it is invalid if it does not. Use the nl parsing logic properly and call nla_parse_deprecated() to fill the nlattrs array and then directly index that array to get the data for the DGID. Just fail if it is NULL. Remove the for loop searching for the nla, and squash the validation and parsing into one function. Fixes an uninitialized read from the stack triggered by userspace if it does not provide the DGID to a kernel initiated RDMA_NL_LS_OP_IP_RESOLVE query. BUG: KMSAN: uninit-value in hex_byte_pack include/linux/hex.h:13 [inline] BUG: KMSAN: uninit-value in ip6_string+0xef4/0x13a0 lib/vsprintf.c:1490 hex_byte_pack include/linux/hex.h:13 [inline] ip6_string+0xef4/0x13a0 lib/vsprintf.c:1490 ip6_addr_string+0x18a/0x3e0 lib/vsprintf.c:1509 ip_addr_string+0x245/0xee0 lib/vsprintf.c:1633 pointer+0xc09/0x1bd0 lib/vsprintf.c:2542 vsnprintf+0xf8a/0x1bd0 lib/vsprintf.c:2930 vprintk_store+0x3ae/0x1530 kernel/printk/printk.c:2279 vprintk_emit+0x307/0xcd0 kernel/printk/printk.c:2426 vprintk_default+0x3f/0x50 kernel/printk/printk.c:2465 vprintk+0x36/0x50 kernel/printk/printk_safe.c:82 _printk+0x17e/0x1b0 kernel/printk/printk.c:2475 ib_nl_process_good_ip_rsep drivers/infiniband/core/addr.c:128 [inline] ib_nl_handle_ip_res_resp+0x963/0x9d0 drivers/infiniband/core/addr.c:141 rdma_nl_rcv_msg drivers/infiniband/core/netlink.c:-1 [inline] rdma_nl_rcv_skb drivers/infiniband/core/netlink.c:239 [inline] rdma_nl_rcv+0xefa/0x11c0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1320 [inline] netlink_unicast+0xf04/0x12b0 net/netlink/af_netlink.c:1346 netlink_sendmsg+0x10b3/0x1250 net/netlink/af_netlink.c:1896 sock_sendmsg_nosec net/socket.c:714 [inline] __sock_sendmsg+0x333/0x3d0 net/socket.c:729 ____sys_sendmsg+0x7e0/0xd80 net/socket.c:2617 ___sys_sendmsg+0x271/0x3b0 net/socket.c:2671 __sys_sendmsg+0x1aa/0x300 net/socket.c:2703 __compat_sys_sendmsg net/compat.c:346 [inline] __do_compat_sys_sendmsg net/compat.c:353 [inline] __se_compat_sys_sendmsg net/compat.c:350 [inline] __ia32_compat_sys_sendmsg+0xa4/0x100 net/compat.c:350 ia32_sys_call+0x3f6c/0x4310 arch/x86/include/generated/asm/syscalls_32.h:371 do_syscall_32_irqs_on arch/x86/entry/syscall_32.c:83 [inline] __do_fast_syscall_32+0xb0/0x150 arch/x86/entry/syscall_32.c:306 do_fast_syscall_32+0x38/0x80 arch/x86/entry/syscall_32.c:331 do_SYSENTER_32+0x1f/0x30 arch/x86/entry/syscall_32.c:3	N/A	More Details
CVE-2025-71095	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix the crash issue for zero copy XDP_TX action There is a crash issue when running zero copy XDP_TX action, the crash log is shown below. [216.122464] Unable to handle kernel paging request at virtual address fffeffff80000000 [216.187524] Internal error: Oops: 0000000096000144 [#1] SMP [216.301694] Call trace: [216.304130] dcache_clean_poc+0x20/0x38 (P) [216.308308] __dma_sync_single_for_device+0x1bc/0x1e0 [216.313351] stmmac_xdp_xmit_xdpf+0x354/0x400 [216.317701] __stmmac_xdp_run_prog+0x164/0x368 [216.322139] stmmac_napi_poll_rxtx+0xba8/0xf00 [216.326576] __napi_poll+0x40/0x218 [216.408054] Kernel panic - not syncing: Oops: Fatal exception in interrupt For XDP_TX action, the xdp_buff is converted to xdp_frame by xdp_convert_buff_to_frame(). The memory type of the resulting xdp_frame depends on the memory type of the xdp_buff. For page pool based xdp_buff it produces xdp_frame with memory type MEM_TYPE_PAGE_POOL. For zero copy XSK pool based xdp_buff it produces xdp_frame with memory type MEM_TYPE_PAGE_ORDER0. However, stmmac_xdp_xmit_back() does not check the memory type and always uses the page pool type, this leads to invalid mappings and causes the crash. Therefore, check the xdp_buff memory type in stmmac_xdp_xmit_back() to fix this issue.	N/A	More Details
CVE-2025-71094	In the Linux kernel, the following vulnerability has been resolved: net: usb: asix: validate PHY address before use The ASIX driver reads the PHY address from the USB device via asix_read_phy_addr(). A malicious or faulty device can return an invalid address (>= PHY_MAX_ADDR), which causes a warning in mdiobus_get_phy(): addr 207 out of range WARNING: drivers/net/phy/mdio_bus.c:76 Validate the PHY address in asix_read_phy_addr() and remove the now-redundant check in ax88172a.c.	N/A	More Details
CVE-2025-71093	In the Linux kernel, the following vulnerability has been resolved: e1000: fix OOB in e1000_tbi_should_accept() In e1000_tbi_should_accept() we read the last byte of the frame via 'data[length - 1]' to evaluate the TBI workaround. If the descriptor- reported length is zero or larger than the actual RX buffer size, this read goes out of bounds and can hit unrelated slab objects. The issue is observed from the NAPI receive path (e1000_clean_rx_irq): == BUG: KASAN: slab-out-of-bounds in e1000_tbi_should_accept+0x610/0x790 Read of size 1 at addr ffff888014114e54 by task sshd/363 CPU: 0 PID: 363 Comm: sshd Not tainted 5.18.0-rc1 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.12.0-59-gc9ba5276e321-prebuilt.qemu.org 04/01/2014 Call Trace: <IRQ> dump_stack_lvl+0x5a/0x74 print_address_description+0x7b/0x440 print_report+0x101/0x200 kasan_report+0xc1/0xf0 e1000_tbi_should_accept+0x610/0x790 e1000_clean_rx_irq+0xa8c/0x1110 e1000_clean+0xde2/0x3c10 __napi_poll+0x98/0x380 net_rx_action+0x491/0xa20 __do_softirq+0x2c9/0x61d do_softirq+0xd1/0x120 </IRQ> <TASK> __local_bh_enable_ip+0xfe/0x130 ip_finish_output2+0x7d5/0xb00 __ip_queue_xmit+0xe24/0x1ab0 __tcp_transmit_skb+0x1bcb/0x3340 tcp_write_xmit+0x175d/0x6bd0 __tcp_push_pending_frames+0x7b/0x280 tcp_sendmsg_locked+0x2e4f/0x32d0 tcp_sendmsg+0x24/0x40 sock_write_iter+0x322/0x430 vfs_write+0x56c/0xa60 ksys_write+0xd1/0x190 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f511b476b10 Code: 73 01 c3 48 8b 0d 88 d3 2b 00 f7 d8 64 89 01 48 83 c8 ff c3 66 0f 1f 44 00 00 83 3d f9 2b 2c 00 00 75 10 b8 01 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 31 c3 48 83 ec 08 e8 8e 9b 01 00 48 89 04 24 RSP: 002b:00007ffc9211d4e8 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 0000000000004024 RCX: 00007f511b476b10 RDX: 0000000000004024 RSI: 0000559a9385962c RDI: 0000000000000003 RBP: 0000559a9383a400 R08: fffffffffffffff0 R09: 0000000000004f00 R10: 0000000000000070 R11: 0000000000000246 R12:	N/A	More Details

	0000000000000000 R13: 00007ffc9211d57f R14: 0000559a9347bde7 R15: 0000000000000003 </TASK> Allocated by task 1: __kasan_krealloc+0x131/0x1c0 krealloc+0x90/0xc0 add_sysfs_param+0xcb/0x8a0 kernel_add_sysfs_param+0x81/0xd4 param_sysfs_builtin+0x138/0x1a6 param_sysfs_init+0x57/0x5b do_one_initcall+0x104/0x250 do_initcall_level+0x102/0x132 do_initcalls+0x46/0x74 kernel_init_freeable+0x28f/0x393 kernel_init+0x14/0x1a0 ret_from_fork+0x22/0x30 The buggy address belongs to the object at ffff888014114000 which belongs to the cache kmalloc-2k of size 2048 The buggy address is located 1620 bytes to the right of 2048-byte region [ffff888014114000, ffff888014114800] The buggy address belongs to the physical page: page:ffffea0000504400 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14110 head:ffffea0000504400 order:3 compound_mapcount:0 compound_pincount:0 flags: 0x100000000010200(slab|head|node=0|zone=1) raw: 0100000000010200 0000000000000000 dead000000000001 ffff888013442000 raw: 0000000000000000 0000000000080008 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected ========== This happens because the TBI check unconditionally dereferences the last byte without validating the reported length first: u8 last_byte = *(data + length - 1); Fix by rejecting the frame early if the length is zero, or if it exceeds adapter->rx_buffer_len. This preserves the TBI workaround semantics for valid frames and prevents touching memory beyond the RX buffer.		
CVE-2025-40978	Stored Cross-Site Scripting (XSS) vulnerability in WorkDo's eCommerceGo SaaS, consisting of a stored XSS due to a lack of proper validation of user input by sending a POST request to ‘/ticket/x/conversion’, using the ‘reply_description’ parameter.	N/A	More Details