SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 February 2026

Generated on 18 February 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-2026-22769	Dell RecoverPoint for Virtual Machines, versions prior to 6.0.3.1 HF1, contain a hardcoded credential vulnerability. This is considered critical as an unauthenticated remote attacker with knowledge of the hardcoded credential could potentially exploit this vulnerability leading to unauthorized access to the underlying operating system and root-level persistence. Dell recommends that customers upgrade or apply one of the remediations as soon as possible.	10.0	More Details
CVE-2025-64075	A path traversal vulnerability in the check_token function of Shenzhen Zhibotong Electronics ZBT WE2001 23.09.27 allows remote attackers to bypass authentication and perform administrative actions by supplying a crafted session cookie value.	10.0	More Details
CVE-2026-2577	The WhatsApp bridge component in Nanobot binds the WebSocket server to all network interfaces (0.0.0.0) on port 3001 by default and does not require authentication for incoming connections. An unauthenticated remote attacker with network access to the bridge can connect to the WebSocket server to hijack the WhatsApp session. This allows the attacker to send messages on behalf of the user, intercept all incoming messages and media in real-time, and capture authentication QR codes.	10.0	More Details
CVE-2026-26216	Crawl4AI versions prior to 0.8.0 contain a remote code execution vulnerability in the Docker API deployment. The /crawl endpoint accepts a hooks parameter containing Python code that is executed using exec(). The __import__ builtin was included in the allowed builtins, allowing unauthenticated remote attackers to import arbitrary modules and execute system commands. Successful exploitation allows full server compromise, including arbitrary command execution, file read and write access, sensitive data exfiltration, and lateral movement within internal networks.	10.0	More Details
CVE-2025-69770	A zip slip vulnerability in the /DesignTools/SkinList.aspx endpoint of MojoPortal CMS v2.9.0.1 allows attackers to execute arbitrary commands via uploading a crafted zip file.	10.0	More Details
CVE-2025-70830	A Server-Side Template Injection (SSTI) vulnerability in the Freemarker template engine of Datart v1.0.0-rc.3 allows authenticated attackers to execute arbitrary code via injecting crafted Freemarker template syntax into the SQL script field.	9.9	More Details
CVE-2026-1357	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Upload in versions up to and including 0.9.123. This is due to improper error handling in the RSA decryption process combined with a lack of path sanitization when writing uploaded files. When the plugin fails to decrypt a session key using openssl_private_decrypt(), it does not terminate execution and instead passes the boolean false value to the phpseclib library's AES cipher initialization. The library treats this false value as a string of null bytes, allowing an attacker to encrypt a malicious payload using a predictable null-byte key. Additionally, the plugin accepts filenames from the decrypted payload without sanitization, enabling directory traversal to escape the protected backup directory. This makes it possible for unauthenticated attackers to upload arbitrary PHP files to publicly accessible directories and achieve Remote Code Execution via the wpvivid_action=send_to_site parameter.	9.8	More Details
CVE-2026-26190	Milvus is an open-source vector database built for generative AI applications. Prior to 2.5.27 and 2.6.10, Milvus exposes TCP port 9091 by default, which enables authentication bypasses. The /expr debug endpoint uses a weak, predictable default authentication token derived from etcd.rootPath (default: by-dev), enabling arbitrary expression evaluation. The full REST API (/api/v1/*) is registered on the metrics/management port without any authentication, allowing unauthenticated access to all business operations including data manipulation and credential management. This vulnerability is fixed in 2.5.27 and 2.6.10.	9.8	More Details

CVE-2025-66277	A link following vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to traverse the file system to unintended locations. We have already fixed the vulnerability in the following versions: QTS 5.2.8.3350 build 20251216 and later QuTS hero h5.3.2.3354 build 20251225 and later QuTS hero h5.2.8.3350 build 20251216 and later	9.8	More Details
CVE-2025-70314	webfsd 1.21 is vulnerable to a Buffer Overflow via a crafted request. This is due to the filename variable	9.8	More Details
CVE-2026-1358	Airleader Master versions 6.381 and prior allow for file uploads without restriction to multiple webpages running maximum privileges. This could allow an unauthenticated user to potentially obtain remote code execution on the server.	9.8	More Details
CVE-2019-25319	Domain Quester Pro 6.02 contains a stack overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the 'Domain Name Keywords' input field to trigger an access violation and execute a bind shell on port 9999.	9.8	More Details
CVE-2019-25321	FTP Navigator 8.03 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload that triggers a buffer overflow when pasted into the Custom Command textbox, enabling remote code execution and launching the calculator as proof of concept.	9.8	More Details
CVE-2019-25327	Prime95 version 29.8 build 6 contains a buffer overflow vulnerability in the user ID input field that allows remote attackers to execute arbitrary code. Attackers can craft a malicious payload and paste it into the PrimeNet user ID and proxy host fields to trigger a bind shell on port 3110.	9.8	More Details
CVE-2019-25337	OwnCloud 8.1.8 contains a username enumeration vulnerability that allows remote attackers to discover user accounts by manipulating the share.php endpoint. Attackers can send crafted GET requests to /index.php/core/ajax/share.php with a wildcard search parameter to retrieve comprehensive user information.	9.8	More Details
CVE-2020-37167	ClamAV ClamBC bytecode interpreter contains a vulnerability in function name processing that allows attackers to manipulate bytecode function names. Attackers can exploit the weak input validation in function name encoding to potentially execute malicious bytecode or cause unexpected behavior in the ClamAV engine.	9.8	More Details
CVE-2025-8572	The Truelysell Core plugin for WordPress is vulnerable to privilege escalation in versions less than, or equal to, 1.8.7. This is due to insufficient validation of the user_role parameter during user registration. This makes it possible for unauthenticated attackers to create accounts with elevated privileges, including administrator access.	9.8	More Details
CVE-2025-69633	A SQL Injection vulnerability in the Advanced Popup Creator (advancedpopupcreator) module for PrestaShop 1.1.26 through 1.2.6 (Fixed in version 1.2.7) allows remote unauthenticated attackers to execute arbitrary SQL queries via the fromController parameter in the popup controller. The parameter is passed unsanitized to SQL queries in classes/AdvancedPopup.php (getPopups() and updateVisits() functions).	9.8	More Details
CVE-2026-1306	The midi-Synth plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type and file extension validation in the 'export' AJAX action in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible granted the attacker can obtain a valid nonce. The nonce is exposed in frontend JavaScript making it trivially accessible to unauthenticated attackers.	9.8	More Details
CVE-2026-1490	The Spam protection, Anti-Spam, FireWall by CleanTalk plugin for WordPress is vulnerable to unauthorized Arbitrary Plugin Installation due to an authorization bypass via reverse DNS (PTR record) spoofing on the 'checkWithoutToken' function in all versions up to, and including, 6.71. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated. Note: This is only exploitable on sites with an invalid API key.	9.8	More Details
CVE-2026-26366	eNet SMART HOME server 2.2.1 and 2.3.1 ships with default credentials (user:user, admin:admin) that remain active after installation and commissioning without enforcing a mandatory password change. Unauthenticated attackers can use these default credentials to gain administrative access to sensitive smart home configuration and control functions.	9.8	More Details
CVE-2026-26369	eNet SMART HOME server 2.2.1 and 2.3.1 contains a privilege escalation vulnerability due to insufficient authorization checks in the setUserGroup JSON-RPC method. A low-privileged user (UG_USER) can send a crafted POST request to /jsonrpc/management specifying their own username to elevate their account to the UG_ADMIN group, bypassing intended access controls and gaining administrative capabilities such as modifying device configurations, network settings, and other smart home system functions.	9.8	More Details
CVE-2026-2550	A vulnerability was found in EFM iptime A6004MX 14.18.2. Affected is the function commit_vpncli_file_upload of the file /cgi/timepro.cgi. The manipulation results in unrestricted upload. The attack may be performed from remote. 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
CVE-2025-15578	Maypole versions from 2.10 through 2.13 for Perl generates session ids insecurely. The session id is seeded with the system time (which is available from HTTP response headers), a call to the built-in rand() function, and the PID.	9.8	More Details
CVE-2026-2439	Concierge::Sessions versions from 0.8.1 before 0.8.5 for Perl generate insecure session ids. The generate_session_id function in Concierge::Sessions::Base defaults to using the uuidgen command to generate a UUID, with a fallback to using Perl's built-in rand function. Neither of these methods are secure, and attackers are able to guess session_ids that can grant them access to systems. Specifically, * There is no warning when uuidgen fails. The software can be quietly using the fallback rand() function with no warnings if the command fails for any reason. * The uuidgen command will generate a time-based UUID if the system does not have a high-quality random number source, because the call does not explicitly specify the --random option. Note that the system time is shared in HTTP responses. * UUIDs are identifiers whose mere possession grants access, as per RFC 9562. * The output of the built-in rand() function is predictable and unsuitable for security applications.	9.8	More Details

CVE-2026-23647	Glory RBG-100 recycler systems using the ISPK-08 software component contain hard-coded operating system credentials that allow remote authentication to the underlying Linux system. Multiple local user accounts, including accounts with administrative privileges, were found to have fixed, embedded passwords. An attacker with network access to exposed services such as SSH may authenticate using these credentials and gain unauthorized access to the system. Successful exploitation allows remote access with elevated privileges and may result in full system compromise.	9.8	More Details
CVE-2025-70981	CordysCRM 1.4.1 is vulnerable to SQL Injection in the employee list query interface (/user/list) via the departmentIds parameter.	9.8	More Details
CVE-2026-26218	newbee-mall includes pre-seeded administrator accounts in its database initialization script. These accounts are provisioned with a predictable default password. Deployments that initialize or reset the database using the provided schema and fail to change the default administrative credentials may allow unauthenticated attackers to log in as an administrator and gain full administrative control of the application.	9.8	More Details
CVE-2020-37153	ASTPP 4.0.1 contains multiple vulnerabilities including cross-site scripting and command injection in SIP device configuration and plugin management interfaces. Attackers can exploit these flaws to inject system commands, hijack administrator sessions, and potentially execute arbitrary code with root permissions through cron task manipulation.	9.8	More Details
CVE-2020-37181	Torrent FLV Converter 1.51 Build 117 contains a stack overflow vulnerability that allows attackers to overwrite Structured Exception Handler (SEH) through a malicious registration code input. Attackers can craft a payload with specific offsets and partial SEH overwrite techniques to potentially execute arbitrary code on vulnerable Windows 32-bit systems.	9.8	More Details
CVE-2025-8025	Missing Authentication for Critical Function, Improper Access Control vulnerability in Dinosoft Business Solutions Dinosoft ERP allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Dinosoft ERP: from < 3.0.1 through 11022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-12059	Insertion of Sensitive Information into Externally-Accessible File or Directory vulnerability in Logo Software Industry and Trade Inc. Logo j-Platform allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Logo j-Platform: from 3.29.6.4 before 3.34.8.9.	9.8	More Details
CVE-2026-2248	METIS WIC devices (versions <= oscore 2.1.234-r18) expose a web-based shell at the /console endpoint that does not require authentication. Accessing this endpoint allows a remote attacker to execute arbitrary operating system commands with root (UID 0) privileges. This results in full system compromise, allowing unauthorized access to modify system configuration, read sensitive data, or disrupt device operations	9.8	More Details
CVE-2026-2249	METIS DFS devices (versions <= oscore 2.1.234-r18) expose a web-based shell at the /console endpoint that does not require authentication. Accessing this endpoint allows a remote attacker to execute arbitrary operating system commands with 'daemon' privileges. This results in the compromise of the software, granting unauthorized access to modify configuration, read and alter sensitive data, or disrupt services.	9.8	More Details
CVE-2026-24789	An unprotected API endpoint allows an attacker to remotely change the device password without providing authentication.	9.8	More Details
CVE-2026-25084	Authentication for ZLAN5143D can be bypassed by directly accessing internal URLs.	9.8	More Details
CVE-2025-69874	nanotar through 0.2.0 has a path traversal vulnerability in parseTar() and parseTarGzip() that allows remote attackers to write arbitrary files outside the intended extraction directory via a crafted tar archive containing path traversal sequence.	9.8	More Details
CVE-2025-70085	An issue was discovered in OpenSatKit 2.2.1. The EventErrStr buffer has a fixed size of 256 bytes. The code uses sprintf to format two filenames (Source1Filename and the string returned by FileUtil_FileStateStr) into this buffer without any length checking and without using bounded format specifiers such as %.*s. If the filename length approaches OS_MAX_PATH_LEN (commonly 64-256 bytes), the combined formatted string together with constant text can exceed 256 bytes, resulting in a stack buffer overflow. Such unsafe sprintf calls are scattered across multiple functions in file.c, including FILE_ConcatenateCmd() and ConcatenateFiles(), all of which fail to validate the output length.	9.8	More Details
CVE-2025-69872	DiskCache (python-diskcache) through 5.6.3 uses Python pickle for serialization by default. An attacker with write access to the cache directory can achieve arbitrary code execution when a victim application reads from the cache.	9.8	More Details
CVE-2025-14014	Unrestricted Upload of File with Dangerous Type vulnerability in NTN Information Processing Services Computer Software Hardware Industry and Trade Ltd. Co. Smart Panel allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Smart Panel: before 20251215.	9.8	More Details
CVE-2020-37176	Torrent 3GP Converter 1.51 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the application's registration dialog to trigger code execution and open the calculator through carefully constructed buffer overflow techniques.	9.8	More Details
CVE-2026-1670	The affected products are vulnerable to an unauthenticated API endpoint exposure, which may allow an attacker to remotely change the "forgot password" recovery email address.	9.8	More Details
CVE-2020-37183	Allok RM RMVB to AVI MPEG DVD Converter 3.6.1217 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload in the License Name input field to trigger a buffer overflow and execute system commands like calc.exe.	9.8	More Details
CVE-2020-37186	Chevereto 3.13.4 Core contains a remote code execution vulnerability that allows attackers to inject malicious code during database configuration installation. Attackers can manipulate the database table prefix parameter to write a PHP shell file and execute arbitrary system commands through a crafted POST request.	9.8	More Details

CVE-2026-26021	set-in provides the set value of nested associative structure given array of keys. A prototype pollution vulnerability exists in the the npm package set-in (>=2.0.1, < 2.0.5). Despite a previous fix that attempted to mitigate prototype pollution by checking whether user input contained a forbidden key, it is still possible to pollute Object.prototype via a crafted input using Array.prototype. This has been fixed in version 2.0.5.	9.8	More Details
CVE-2025-67135	Weak Security in the PF-50 1.2 keyfob of PGST PG107 Alarm System 1.25.05.hf allows attackers to compromise access control via a code replay attack.	9.8	More Details
CVE-2025-10969	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Farktor Software E-Commerce Services Inc. E-Commerce Package allows Blind SQL Injection.This issue affects E-Commerce Package: through 27112025.	9.8	More Details
CVE-2026-1729	The AdForest theme for WordPress is vulnerable to authentication bypass in all versions up to, and including, 6.0.12. This is due to the plugin not properly verifying a user's identity prior to authenticating them through the 'sb_login_user_with_otp_fun' function. This makes it possible for unauthenticated attackers to log in as arbitrary users, including administrators.	9.8	More Details
CVE-2025-14892	The Prime Listing Manager WordPress plugin through 1.1 allows an attacker to gain administrative access without having any kind of account on the targeted site and perform unauthorized actions due to a hardcoded secret.	9.8	More Details
CVE-2020-37184	Allok Video Converter 4.6.1217 contains a stack overflow vulnerability in the License Name input field that allows attackers to execute arbitrary code. Attackers can craft a specially designed payload to overwrite SEH handlers and execute system commands by injecting malicious bytecode into the input field.	9.8	More Details
CVE-2026-22208	OpenS100 (the reference implementation S-100 viewer) prior to commit 753cf29 contain a remote code execution vulnerability via an unrestricted Lua interpreter. The Portrayal Engine initializes Lua using luaL_openlibs() without sandboxing or capability restrictions, exposing standard libraries such as 'os' and 'io' to untrusted portrayal catalogues. An attacker can provide a malicious S-100 portrayal catalogue containing Lua scripts that execute arbitrary commands with the privileges of the OpenS100 process when a user imports the catalogue and loads a chart.	9.6	More Details
CVE-2025-8668	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in E-Kalite Software Hardware Engineering Design and Internet Services Industry and Trade Ltd. Co. Turboard allows Reflected XSS.This issue affects Turboard: from 2025.07 through 11022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.4	More Details
CVE-2025-15573	The affected devices do not validate the server certificate when connecting to the SolaX Cloud MQTTS server hosted in the Alibaba Cloud (mqtt001.solaxcloud.com, TCP 8883). This allows attackers in a man-in-the-middle position to act as the legitimate MQTT server and issue arbitrary commands to devices.	9.4	More Details
CVE-2025-32058	The Infotainment ECU manufactured by Bosch uses a RH850 module for CAN communication. RH850 is connected to infotainment over the INC interface through a custom protocol. There is a vulnerability during processing requests of this protocol on the V850 side which allows an attacker with code execution on the infotainment main SoC to perform code execution on the RH850 module and subsequently send arbitrary CAN messages over the connected CAN bus. First identified on Nissan Leaf ZE1 manufactured in 2020.	9.3	More Details
CVE-2026-26219	newbee-mall stores and verifies user passwords using an unsalted MD5 hashing algorithm. The implementation does not incorporate per-user salts or computational cost controls, enabling attackers who obtain password hashes through database exposure, backup leakage, or other compromise vectors to rapidly recover plaintext credentials via offline attacks.	9.1	More Details
CVE-2025-65717	An issue in Visual Studio Code Extensions Live Server v5.7.9 allows attackers to exfiltrate files via user interaction with a crafted HTML page.	9.1	More Details
CVE-2026-25227	authentik is an open-source identity provider. From 2021.3.1 to before 2025.8.6, 2025.10.4, and 2025.12.4, when using delegated permissions, a User that has the permission Can view * Property Mapping or Can view Expression Policy is able to execute arbitrary code within the authentik server container through the test endpoint, which is intended to preview how a property mapping/policy works. authentik 2025.8.6, 2025.10.4, and 2025.12.4 fix this issue.	9.1	More Details
CVE-2025-65753	An issue in the TLS certification mechanism of Guardian Gryphon v01.06.0006.22 allows attackers to execute commands as root.	9.0	More Details
CVE-2026-20677	A race condition was addressed with improved handling of symbolic links. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. A shortcut may be able to bypass sandbox restrictions.	9.0	More Details
CVE-2025-69634	Cross Site Request Forgery vulnerability in Dolibarr ERP & CRM v.22.0.9 allows a remote attacker to escalate privileges via the notes field in perms.php NOTE: this is disputed by a third party who indicates that exploitation can only occur if an unprivileged user knows the token of an admin user.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-2004	Missing validation of type of input in PostgreSQL intarray extension selectivity estimator function allows an object creator to execute arbitrary code as the operating system user running the database. Versions before PostgreSQL 18.2, 17.8, 16.12, 15.16, and 14.21 are affected.	8.8	More Details
CVE-2025-70866	LavaLite CMS 10.1.0 is vulnerable to Incorrect Access Control. An authenticated user with low-level privileges (User role) can directly access the admin backend by logging in through /admin/login. The vulnerability exists because the admin and user authentication guards share the same user provider without role-based access control verification.	8.8	More Details

CVE-2025-61880	In Infoblox NIOS through 9.0.7, insecure deserialization can result in remote code execution.	8.8	More Details
CVE-2025-15096	The 'Videospirecore Theme Plugin' plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.0.6. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	8.8	More Details
CVE-2026-2441	Use after free in CSS in Google Chrome prior to 145.0.7632.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-50620	Unrestricted Upload of File with Dangerous Type vulnerabilities exist in the rich text editor and document manage components in CIPPlanner CIPAce before 9.17. An authorized user can upload executable files when inserting images in the rich text editor, and upload executable files when uploading files on the document management page. Those executables can be executed if they are not stored in a shared directory or if the storage directory has executed permissions.	8.8	More Details
CVE-2026-2447	Heap buffer overflow in libvpx. This vulnerability affects Firefox < 147.0.4, Firefox ESR < 140.7.1, Firefox ESR < 115.32.1, Thunderbird < 140.7.2, and Thunderbird < 147.0.2.	8.8	More Details
CVE-2025-65716	An issue in Visual Studio Code Extensions Markdown Preview Enhanced v0.8.18 allows attackers to execute arbitrary code via uploading a crafted .Md file.	8.8	More Details
CVE-2025-30276	An out-of-bounds write vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify or corrupt memory. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.8	More Details
CVE-2026-25922	authentik is an open-source identity provider. Prior to 2025.8.6, 2025.10.4, and 2025.12.4, when using a SAML Source that has the option Verify Assertion Signature under Verification Certificate enabled and not Verify Response Signature, or does not have the Encryption Certificate setting under Advanced Protocol settings configured, it was possible for an attacker to inject a malicious assertion before the signed assertion that authentik would use instead. authentik 2025.8.6, 2025.10.4, and 2025.12.4 fix this issue.	8.8	More Details
CVE-2025-57707	An improper neutralization of directives in statically saved code ('Static Code Injection') vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to access restricted data / files. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5166 and later	8.8	More Details
CVE-2026-2001	The WowRevenue plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check in the 'Notice::install_activate_plugin' function in all versions up to, and including, 2.1.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to install arbitrary plugins on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2026-1618	Authentication Bypass Using an Alternate Path or Channel vulnerability in Universal Software Inc. FlexCity/Kiosk allows Privilege Escalation.This issue affects FlexCity/Kiosk: from 1.0 before 1.0.36.	8.8	More Details
CVE-2025-14349	Privilege Defined With Unsafe Actions, Missing Authentication for Critical Function vulnerability in Universal Software Inc. FlexCity/Kiosk allows Accessing Functionality Not Properly Constrained by ACLs, Privilege Escalation.This issue affects FlexCity/Kiosk: from 1.0 before 1.0.36.	8.8	More Details
CVE-2025-12062	The WP Maps – Store Locator,Google Maps,OpenStreetMap,Mapbox,Listing,Directory & Filters plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.8.6 via the fc_load_template function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to include and execute arbitrary .html files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .html file types can be uploaded and included.	8.8	More Details
CVE-2026-20667	A logic issue was addressed with improved checks. This issue is fixed in watchOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 26.3 and iPadOS 26.3. An app may be able to break out of its sandbox.	8.8	More Details
CVE-2026-0910	The wpForo Forum plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.4.13 via deserialization of untrusted input in the 'wpforo_display_array_data' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	8.8	More Details
CVE-2026-2616	A vulnerability has been found in Beetel 777VR1 up to 01.00.09. The impacted element is an unknown function of the component Web Management Interface. The manipulation leads to hard-coded credentials. The attack needs to be initiated within the local network. The exploit has been disclosed to the public and may be used. It is advisable to modify the configuration settings. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-70397	jizhicms 2.5.6 is vulnerable to SQL Injection in Article/deleteAll and Extmolds/deleteAll via the data parameter.	8.8	More Details
CVE-2026-23595	An authentication bypass in the application API allows an unauthorized administrative account to be created. A remote attacker could exploit this vulnerability to create privileged user accounts. Successful exploitation could allow an attacker to gain administrative access, modify system configurations, and access or manipulate sensitive data.	8.8	More Details

CVE-2024-36324	Improper input validation in AMD Graphics Driver could allow an attacker to supply a specially crafted pointer, potentially leading to arbitrary code execution.	8.8	More Details
CVE-2019-25318	AVS Audio Converter 9.1.2.600 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by manipulating the output folder text input. Attackers can craft a malicious payload that overwrites stack memory and triggers a bind shell on port 9999 when the 'Browse' button is clicked.	8.8	More Details
CVE-2025-70828	An issue in Datart v1.0.0-rc.3 allows attackers to execute arbitrary code via the url parameter in the JDBC configuration	8.8	More Details
CVE-2025-65480	An issue was discovered in Pacom Unison Client 5.13.1. Authenticated users can inject malicious scripts in the Report Templates which are executed when certain script conditions are fulfilled, leading to Remote Code Execution.	8.8	More Details
CVE-2026-26056	Yoke is a Helm-inspired infrastructure-as-code (IaC) package deployer. In 0.19.0 and earlier, a vulnerability exists in the Air Traffic Controller (ATC) component of Yoke. It allows users with CR create/update permissions to execute arbitrary WASM code in the ATC controller context by injecting a malicious URL through the overrides.yoke.cd/flight annotation. The ATC controller downloads and executes the WASM module without proper URL validation, enabling attackers to create arbitrary Kubernetes resources or potentially escalate privileges to cluster-admin level.	8.8	More Details
CVE-2026-26020	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to 0.6.48, an authenticated user could achieve Remote Code Execution (RCE) on the backend server by embedding a disabled block inside a graph. The BlockInstallationBlock — a development tool capable of writing and importing arbitrary Python code — was marked disabled=True, but graph validation did not enforce this flag. This allowed any authenticated user to bypass the restriction by including the block as a node in a graph, rather than calling the block's execution endpoint directly (which did enforce the flag). This vulnerability is fixed in 0.6.48.	8.8	More Details
CVE-2024-55270	phpgurukul Student Management System 1.0 is vulnerable to SQL Injection in studentms/admin/search.php via the searchdata parameter.	8.8	More Details
CVE-2026-2313	Use after free in CSS in Google Chrome prior to 145.0.7632.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-2314	Heap buffer overflow in Codecs in Google Chrome prior to 145.0.7632.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-2315	Inappropriate implementation in WebGPU in Google Chrome prior to 145.0.7632.45 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-0969	The serialize function used to compile MDX in next-mdx-remote is vulnerable to arbitrary code execution due to insufficient sanitization of MDX content. This vulnerability, CVE-2026-0969, is fixed in next-mdx-remote 6.0.0.	8.8	More Details
CVE-2025-15157	The Starfish Review Generation & Marketing for WordPress plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'srm_restore_options_defaults' function in all versions up to, and including, 3.1.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	8.8	More Details
CVE-2026-2321	Use after free in Ozone in Google Chrome prior to 145.0.7632.45 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2025-32061	The specific flaw exists within the Bluetooth stack developed by Alps Alpine of the Infotainment ECU manufactured by Bosch. The issue results from the lack of proper boundary validation of user-supplied data, which can result in a stack-based buffer overflow when receiving a specific packet on the established upper layer L2CAP channel. An attacker can leverage this vulnerability to obtain remote code execution on the Infotainment ECU with root privileges. First identified on Nissan Leaf ZE1 manufactured in 2020.	8.8	More Details
CVE-2025-13689	IBM DataStage on Cloud Pak for Data could allow an authenticated user to execute arbitrary commands and gain access to sensitive information due to unrestricted file uploads.	8.8	More Details
CVE-2026-1104	The FastDup – Fastest WordPress Migration & Duplicator plugin for WordPress is vulnerable to unauthorized backup creation and download due to a missing capability check on REST API endpoints in all versions up to, and including, 2.7.1. This makes it possible for authenticated attackers, with Contributor-level access and above, to create and download full-site backup archives containing the entire WordPress installation, including database exports and configuration files.	8.8	More Details
CVE-2026-26119	Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2025-32059	The specific flaw exists within the Bluetooth stack developed by Alps Alpine of the Infotainment ECU manufactured by Bosch. The issue results from the lack of proper boundary validation of user-supplied data, which can result in a stack-based buffer overflow when receiving a specific packet on the established upper layer L2CAP channel. An attacker can leverage this vulnerability to obtain remote code execution on the Infotainment ECU with root privileges. First identified on Nissan Leaf ZE1	8.8	More Details

	manufactured in 2020.		
CVE-2025-32062	The specific flaw exists within the Bluetooth stack developed by Alps Alpine of the Infotainment ECU manufactured by Bosch. The issue results from the lack of proper boundary validation of user-supplied data, which can result in a stack-based buffer overflow when receiving a specific packet on the established upper layer L2CAP channel. An attacker can leverage this vulnerability to obtain remote code execution on the Infotainment ECU with root privileges. First identified on Nissan Leaf ZE1 manufactured in 2020.	8.8	More Details
CVE-2026-2005	Heap buffer overflow in PostgreSQL pgcrypto allows a ciphertext provider to execute arbitrary code as the operating system user running the database. Versions before PostgreSQL 18.2, 17.8, 16.12, 15.16, and 14.21 are affected.	8.8	More Details
CVE-2026-2006	Missing validation of multibyte character length in PostgreSQL text manipulation allows a database user to issue crafted queries that achieve a buffer overrun. That suffices to execute arbitrary code as the operating system user running the database. Versions before PostgreSQL 18.2, 17.8, 16.12, 15.16, and 14.21 are affected.	8.8	More Details
CVE-2026-1750	The Ecwid by Lightspeed Ecommerce Shopping Cart plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 7.0.7. This is due to a missing capability check in the 'save_custom_user_profile_fields' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to supply the 'ec_store_admin_access' parameter during a profile update and gain store manager access to the site.	8.8	More Details
CVE-2026-1560	The Custom Block Builder – Lazy Blocks plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.2.0 via multiple functions in the 'LazyBlocks_Blocks' class. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.	8.8	More Details
CVE-2026-26368	eNet SMART HOME server 2.2.1 and 2.3.1 contains a missing authorization vulnerability in the resetUserPassword JSON-RPC method that allows any authenticated low-privileged user (UG_USER) to reset the password of arbitrary accounts, including those in the UG_ADMIN and UG_SUPER_ADMIN groups, without supplying the current password or having sufficient privileges. By sending a crafted JSON-RPC request to /jsonrpc/management, an attacker can overwrite existing credentials, resulting in direct account takeover with full administrative access and persistent privilege escalation.	8.8	More Details
CVE-2026-26234	JUNG Smart Visu Server 1.1.1050 contains a request header manipulation vulnerability that allows unauthenticated attackers to override request URLs by injecting arbitrary values in the X-Forwarded-Host header. Attackers can manipulate proxied requests to generate tainted responses, enabling cache poisoning, potential phishing, and redirecting users to malicious domains.	8.8	More Details
CVE-2024-50619	Vulnerabilities in the My Account and User Management components in CIPPlanner CIPAce before 9.17 allows attackers to escalate their access levels. A low-privileged authenticated user can gain access to other people's accounts by tampering with the client's user id to change their account information. A low-privileged authenticated user can elevate his or her system privileges by modifying the information of a user role that is disabled in the client.	8.8	More Details
CVE-2026-2630	A Command Injection vulnerability exists where an authenticated, remote attacker could execute arbitrary code on the underlying server where Tenable Security Center is hosted.	8.8	More Details
CVE-2026-25759	Statmatic is a Laravel and Git powered content management system (CMS). From 6.0.0 to before 6.2.3, a stored XSS vulnerability in content titles allows authenticated users with content creation permissions to inject malicious JavaScript that executes when viewed by higher-privileged users. Malicious user must have an account with control panel access and content creation permissions. This vulnerability can be exploited to allow super admin accounts to be created. This has been fixed in 6.2.3.	8.7	More Details
CVE-2025-67905	Malwarebytes AdwCleaner before v.8.7.0 runs as Administrator and performs an insecure log file delete operation in which the target location is user-controllable, allowing a non-admin user to escalate privileges to SYSTEM via a symbolic link, a related issue to CVE-2023-28892. To exploit this, an attacker must create a file in a given folder path and intercept the application log file deletion flow.	8.7	More Details
CVE-2026-2101	A Reflected Cross-site Scripting (XSS) vulnerability affecting ENOVIAvpm Web Access from ENOVIAvpm Version 1 Release 16 through ENOVIAvpm Version 1 Release 19 allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2026-26217	Crawl4AI versions prior to 0.8.0 contain a local file inclusion vulnerability in the Docker API deployment. The /execute_js, /screenshot, /pdf, and /html endpoints accept file:// URLs, allowing unauthenticated remote attackers to read arbitrary files from the server filesystem. An attacker can access sensitive files such as /etc/passwd, /etc/shadow, application configuration files, and environment variables via /proc/self/environ, potentially exposing credentials, API keys, and internal application structure.	8.6	More Details
CVE-2025-7631	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tumeva Internet Technologies Software Information Advertising and Consulting Services Trade Ltd. Co. Tumeva News Software allows SQL Injection.This issue affects Tumeva News Software: through 17022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.6	More Details
CVE-2026-25748	authentik is an open-source identity provider. Prior to 2025.10.4 and 2025.12.4, with a malformed cookie it was possible to bypass authentication when using forward authentication in the authentik Proxy Provider when used in conjunction with Traefik or Caddy as reverse proxy. When a malicious cookie was used, none of the authentik-specific X-Authentik-* headers were set which depending on application can grant access to an attacker. authentik 2025.10.4 and 2025.12.4 fix this issue.	8.6	More Details
CVE-2019-25332	FTP Commander Pro 8.03 contains a local stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting the EIP register through a custom command input. Attackers can craft a malicious payload of 4108 bytes to overwrite memory and execute shellcode, demonstrating remote code execution potential.	8.4	More Details
CVE-2019-25331	AVS Audio Converter 9.1 contains a local buffer overflow vulnerability that allows local attackers to overwrite CPU registers by manipulating the 'Exit folder' input field. Attackers can craft a specially designed text file with 264 bytes of padding followed by register overwrite values to compromise the application and potentially execute arbitrary code.	8.4	More Details
CVE-	SpotAuditor 5.3.2 contains a local buffer overflow vulnerability in the Base64 Encrypted Password tool that allows attackers to		

2019-25336	execute arbitrary code by crafting a malicious payload. Attackers can generate a specially crafted Base64 encoded payload to trigger a Structured Exception Handler (SEH) overwrite and execute shellcode on the vulnerable system.	8.4	More Details
CVE-2025-54756	BrightSign players running BrightSign OS series 4 prior to v8.5.53.1 or series 5 prior to v9.0.166 use a default password that is guessable with knowledge of the device information. The latest release fixes this issue for new installations; users of old installations are encouraged to change all default passwords.	8.4	More Details
CVE-2026-25924	Kanboard is project management software focused on Kanban methodology. Prior to 1.2.50, a security control bypass vulnerability in Kanboard allows an authenticated administrator to achieve full Remote Code Execution (RCE). Although the application correctly hides the plugin installation interface when the PLUGIN_INSTALLER configuration is set to false, the underlying backend endpoint fails to verify this security setting. An attacker can exploit this oversight to force the server to download and install a malicious plugin, leading to arbitrary code execution. This vulnerability is fixed in 1.2.50.	8.4	More Details
CVE-2026-1619	Authorization Bypass Through User-Controlled Key vulnerability in Universal Software Inc. FlexCity/Kiosk allows Exploitation of Trusted Identifiers.This issue affects FlexCity/Kiosk: from 1.0 before 1.0.36.	8.3	More Details
CVE-2025-10174	Cleartext Transmission of Sensitive Information vulnerability in Pan Software & Information Technologies Ltd. PanCafe Pro allows Flooding.This issue affects PanCafe Pro: from < 3.3.2 through 23092025.	8.3	More Details
CVE-2025-10913	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saastech Cleaning and Internet Services Inc. TemizlikYolda allows Cross-Site Scripting (XSS).This issue affects TemizlikYolda: through 11022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.3	More Details
CVE-2026-2007	Heap buffer overflow in PostgreSQL pg_trgm allows a database user to achieve unknown impacts via a crafted input string. The attacker has limited control over the byte patterns to be written, but we have not ruled out the viability of attacks that lead to privilege escalation. PostgreSQL 18.1 and 18.0 are affected.	8.2	More Details
CVE-2019-25325	Thrive Smart Home 1.1 contains an SQL injection vulnerability in the checklogin.php endpoint that allows unauthenticated attackers to bypass authentication by manipulating the 'user' POST parameter. Attackers can inject malicious SQL code like ' or 1=1# to manipulate login queries and gain unauthorized access to the application.	8.2	More Details
CVE-2026-23857	Dell Update Package (DUP) Framework, versions 23.12.00 through 24.12.00, contains an Improper Handling of Insufficient Permissions or Privileges vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	8.2	More Details
CVE-2025-9986	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Vadi Corporate Information Systems Ltd. Co. DIGIKENT allows Excavation.This issue affects DIGIKENT: through 13092025.	8.2	More Details
CVE-2025-13002	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Farktor Software E-Commerce Services Inc. E-Commerce Package allows Cross-Site Scripting (XSS).This issue affects E-Commerce Package: through 27112025.	8.2	More Details
CVE-2025-13691	IBM DataStage on Cloud Pak for Data 5.1.2 through 5.3.0 returns sensitive information in an HTTP response that could be used to impersonate other users in the system.	8.1	More Details
CVE-2025-57709	A buffer overflow vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2025-52870	A buffer overflow vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2026-2564	A security flaw has been discovered in Intelbras VIP 3260 Z IA 2.840.00IB005.0.T. Affected by this vulnerability is an unknown functionality of the file /OutsideCmd. The manipulation results in weak password recovery. It is possible to launch the attack remotely. Attacks of this nature are highly complex. The exploitation appears to be difficult. It is recommended to upgrade the affected component.	8.1	More Details
CVE-2025-48724	A buffer overflow vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2025-52869	A buffer overflow vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2025-52868	A buffer overflow vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2025-48725	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: QuTS hero h5.3.2.3354 build 20251225 and later	8.1	More Details
CVE-2026-24853	Caido is a web security auditing toolkit. Prior to 0.55.0, Caido blocks non whitelisted domains to reach out through the 8080 port, and shows Host/IP is not allowed to connect to Caido on all endpoints. But this is bypassable by injecting a X-Forwarded-Host: 127.0.0.1:8080 header. This vulnerability is fixed in 0.55.0.	8.1	More Details
	lakeFS is an open-source tool that transforms object storage into a Git-like repositories. Prior to 1.77.0, the local block adapter		

CVE-2026-26187	(pkg/block/local/adapter.go) allows authenticated users to read and write files outside their designated storage boundaries. The verifyRelPath function used strings.HasPrefix() to verify that requested paths fall within the configured storage directory. This check was insufficient because it validated only the path prefix without requiring a path separator, allowing access to sibling directories with similar names. Also, the adapter verified that resolved paths stayed within the adapter's base path, but did not verify that object identifiers stayed within their designated storage namespace. This allowed attackers to use path traversal sequences in the object identifier to access files in other namespaces. Fixed in version v1.77.0.	8.1	More Details
CVE-2025-48723	A buffer overflow vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2026-2144	The Magic Login Mail or QR Code plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.05. This is due to the plugin storing the magic login QR code image with a predictable, static filename (QR_Code.png) in the publicly accessible WordPress uploads directory during the email sending process. The file is only deleted after wp_mail() completes, creating an exploitable race condition window. This makes it possible for unauthenticated attackers to trigger a login link request for any user, including administrators, and then exploit the race condition between QR code file creation and deletion to obtain the login URL encoded in the QR code, thereby gaining unauthorized access to the targeted user's account.	8.1	More Details
CVE-2025-69871	A race condition vulnerability exists in MedusaJS Medusa v2.12.2 and earlier in the registerUsage() function of the promotion module. The function performs a non-atomic read-check-update operation when enforcing promotion usage limits. This allows unauthenticated remote attackers to bypass usage limits by sending concurrent checkout requests, resulting in unlimited redemptions of limited-use promotional codes and potential financial loss.	8.1	More Details
CVE-2025-65128	A missing authentication mechanism in the web management API components of Shenzhen Zhibotong Electronics ZBT WE2001 23.09.27 allows unauthenticated attackers on the local network to modify router and network configurations. By invoking operations whose names end with "*_nocommit" and supplying the parameters expected by the invoked function, an attacker can change configuration data, including SSID, Wi-Fi credentials, and administrative passwords, without authentication or an existing session.	8.1	More Details
CVE-2025-30269	A use of externally-controlled format string vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to obtain secret data or modify memory. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	8.1	More Details
CVE-2025-7659	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an unauthenticated user to steal tokens and access private repositories by abusing incomplete validation in the Web IDE.	8.0	More Details
CVE-2026-2361	PostgreSQL Anonymizer contains a vulnerability that allows a user to gain superuser privileges by creating a temporary view based on a function containing malicious code. When the anon.get_tablesample_ratio function is then called, the malicious code is executed with superuser privileges. This privilege elevation can be exploited by users having the CREATE privilege in PostgreSQL 15 and later. The risk is higher with PostgreSQL 14 or with instances upgraded from PostgreSQL 14 or a prior version because the creation permission on the public schema is granted by default. The problem is resolved in PostgreSQL Anonymizer 3.0.1 and further versions	8.0	More Details
CVE-2026-2360	PostgreSQL Anonymizer contains a vulnerability that allows a user to gain superuser privileges by creating a custom operator in the public schema and place malicious code in that operator. This operator will later be executed with superuser privileges when the extension is created. The risk is higher with PostgreSQL 14 or with instances upgraded from PostgreSQL 14 or a prior version. With PostgreSQL 15 and later, the creation permission on the public schema is revoked by default and this exploit can only be achieved if a superuser adds a new schema in her/his own search_path and grants the CREATE privilege on that schema to untrusted users, both actions being clearly discouraged by the PostgreSQL documentation. The problem is resolved in PostgreSQL Anonymizer 3.0.1 and further versions	8.0	More Details
CVE-2026-26268	Cursor is a code editor built for programming with AI. Sandbox escape via writing .git configuration was possible in versions prior to 2.5. A malicious agent (ie prompt injection) could write to improperly protected .git settings, including git hooks, which may cause out-of-sandbox RCE next time they are triggered. No user interaction was required as Git executes these commands automatically. Fixed in version 2.5.	8.0	More Details
CVE-2019-25345	Realtek IIS Codec Service 6.4.10041.133 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in the service configuration to inject malicious executables and escalate privileges on the system.	7.8	More Details
CVE-2026-2627	A security flaw has been discovered in Softland FBackup up to 9.9. This impacts an unknown function in the library C:\Program Files\Common Files\microsoft shared\ink\HID.dll of the component Backup/Restore. The manipulation results in link following. The attack needs to be approached locally. 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.	7.8	More Details
CVE-2026-23856	Dell iDRAC Service Module (iSM) for Windows, versions prior to 6.0.3.1, and Dell iDRAC Service Module (iSM) for Linux, versions prior to 5.4.1.1, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.8	More Details
CVE-2026-20614	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3, macOS Sonoma 14.8.4. An app may be able to gain root privileges.	7.8	More Details
CVE-2026-20610	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Tahoe 26.3. An app may be able to gain root privileges.	7.8	More Details
CVE-2019-25343	NextVPN 4.10 contains an insecure file permissions vulnerability that allows local users to modify executable files with full access rights. Attackers can replace system executables with malicious files to gain SYSTEM or Administrator privileges through unauthorized file modification.	7.8	More Details

CVE-2019-25306	BlackMoon FTP Server 3.1.2.1731 contains an unquoted service path vulnerability that allows local users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted binary path in the service configuration to insert malicious code that would execute with LocalSystem account permissions during service startup.	7.8	More Details
CVE-2026-23648	Glory RBG-100 recycler systems using the ISPK-08 software component contain multiple system binaries with overly permissive file permissions. Several binaries executed by the root user are writable and executable by unprivileged local users. An attacker with local access can replace or modify these binaries to execute arbitrary commands with root privileges, enabling local privilege escalation.	7.8	More Details
CVE-2019-25310	ActiveFax Server 6.92 Build 0316 contains an unquoted service path vulnerability in the ActiveFaxServiceNT service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path to inject malicious executables that will be launched with elevated administrative privileges.	7.8	More Details
CVE-2019-25307	WorkgroupMail 7.5.1 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 to inject malicious executables that will be run with LocalSystem privileges during service startup.	7.8	More Details
CVE-2025-48503	A DLL hijacking vulnerability in the AMD Software Installer could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	7.8	More Details
CVE-2019-25308	Mikogo 5.2.2.150317 contains an unquoted service path vulnerability in the Mikogo-Service Windows service configuration. Attackers can exploit the unquoted path to inject and execute malicious code with LocalSystem privileges by placing executable files in specific path locations.	7.8	More Details
CVE-2019-25344	Wondershare MobileGo 8.5.0 contains an insecure file permissions vulnerability that allows local users to modify executable files in the application directory. Attackers can replace the original MobileGo.exe with a malicious executable to create a new user account and add it to the Administrators group with full system access.	7.8	More Details
CVE-2019-25309	Zilab Remote Console Server 3.2.9 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 in the service configuration to inject malicious executables that will be run with LocalSystem permissions.	7.8	More Details
CVE-2025-70083	An issue was discovered in OpenSatKit 2.2.1. The DirName field in the telecommand is provided by the ground segment and must be treated as untrusted input. The program copies DirName into the local buffer DirWithSep using strcpy. The size of this buffer is OS_MAX_PATH_LEN. If the length of DirName is greater than or equal to OS_MAX_PATH_LEN, a stack buffer overflow occurs, overwriting adjacent stack memory. The path length check (FileUtil_AppendPathSep) is performed after the strcpy operation, meaning the validation occurs too late and cannot prevent the overflow.	7.8	More Details
CVE-2026-20700	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An attacker with memory write capability may be able to execute arbitrary code. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26. CVE-2025-14174 and CVE-2025-43529 were also issued in response to this report.	7.8	More Details
CVE-2026-20658	A package validation issue was addressed by blocking the vulnerable package. This issue is fixed in macOS Tahoe 26.3. An app may be able to gain root privileges.	7.8	More Details
CVE-2026-20615	A path handling issue was addressed with improved validation. This issue is fixed in iOS 26.3 and iPadOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, visionOS 26.3. An app may be able to gain root privileges.	7.8	More Details
CVE-2026-26208	ADB Explorer is a fluent UI for ADB on Windows. Prior to Beta 0.9.26020, ADB Explorer is vulnerable to Insecure Deserialization leading to Remote Code Execution. The application attempts to deserialize the App.txt settings file using Newtonsoft.Json with TypeNameHandling set to Objects. This allows an attacker to supply a crafted JSON file containing a gadget chain (e.g., ObjectDataProvider) to execute arbitrary code when the application launches and subsequently saves its settings. This vulnerability is fixed in Beta 0.9.26020.	7.8	More Details
CVE-2026-1334	An Out-Of-Bounds Read vulnerability affecting the EPRT file reading procedure in SOLIDWORKS eDrawings from Release SOLIDWORKS Desktop 2025 through Release SOLIDWORKS Desktop 2026 could allow an attacker to execute arbitrary code while opening a specially crafted EPRT file.	7.8	More Details
CVE-2024-56808	A command injection vulnerability has been reported to affect Media Streaming add-on. If an attacker gains local network access who have also gained a user account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following version: Media Streaming add-on 500.1.1.6 (2024/08/02) and later	7.8	More Details
CVE-2026-1333	A Use of Uninitialized Variable vulnerability affecting the EPRT file reading procedure in SOLIDWORKS eDrawings from Release SOLIDWORKS Desktop 2025 through Release SOLIDWORKS Desktop 2026 could allow an attacker to execute arbitrary code while opening a specially crafted EPRT file.	7.8	More Details
CVE-2026-20626	This issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 26.3 and iPadOS 26.3, macOS Tahoe 26.3, visionOS 26.3. A malicious app may be able to gain root privileges.	7.8	More Details
CVE-2025-63421	An issue in filosoft Comerc.32 Commercial Invoicing v.16.0.0.3 allows a local attacker to execute arbitrary code via the comeinst.exe file	7.8	More Details
CVE-2026-1335	An Out-Of-Bounds Write vulnerability affecting the EPRT file reading procedure in SOLIDWORKS eDrawings from Release SOLIDWORKS Desktop 2025 through Release SOLIDWORKS Desktop 2026 could allow an attacker to execute arbitrary code while opening a specially crafted EPRT file.	7.8	More Details

CVE-2026-25991	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.5.1, there is a Blind Server-Side Request Forgery (SSRF) vulnerability in the Cookmate recipe import feature of Tandoor Recipes. The application fails to validate the destination URL after following HTTP redirects, allowing any authenticated user (including standard users without administrative privileges) to force the server to connect to arbitrary internal or external resources. The vulnerability lies in cookbook/integration/cookmate.py, within the Cookmate integration class. This vulnerability can be leveraged to scan internal network ports, access cloud instance metadata (e.g., AWS/GCP Metadata Service), or disclose the server's real IP address. This vulnerability is fixed in 2.5.1.	7.7	More Details
CVE-2026-2592	The Zarinpal Gateway for WooCommerce plugin for WordPress is vulnerable to Improper Access Control to Payment Status Update in all versions up to and including 5.0.16. This is due to the payment callback handler 'Return_from_ZarinPal_Gateway' failing to validate that the authority token provided in the callback URL belongs to the specific order being marked as paid. This makes it possible for unauthenticated attackers to potentially mark orders as paid without proper payment by reusing a valid authority token from a different transaction of the same amount.	7.7	More Details
CVE-2025-61879	In Infoblox NIOS through 9.0.7, a High-Privileged User Can Trigger an Arbitrary File Write via the Account Creation Mechanism.	7.7	More Details
CVE-2026-20620	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3, macOS Sonoma 14.8.4. An attacker may be able to cause unexpected system termination or read kernel memory.	7.7	More Details
CVE-2026-2469	Versions of the package directorytree/imapengine before 1.22.3 are vulnerable to Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') via the id() function in ImapConnection.php due to improperly escaping user input before including it in IMAP ID commands. This allows attackers to read or delete victim's emails, terminate the victim's session or execute any valid IMAP command on victim's mailbox by including quote characters " or CRLF sequences \r\n in the input.	7.6	More Details
CVE-2025-64487	Outline is a service that allows for collaborative documentation. Prior to 1.1.0, a privilege escalation vulnerability exists in the Outline document management system due to inconsistent authorization checks between user and group membership management endpoints. This vulnerability is fixed in 1.1.0.	7.6	More Details
CVE-2026-1046	Mattermost Desktop App versions <=6.0 6.2.0 5.2.13.0 fail to validate help links which allows a malicious Mattermost server to execute arbitrary executables on a user’s system via the user clicking on certain items in the Help menu Mattermost Advisory ID: MMSA-2026-00577	7.6	More Details
CVE-2026-26010	OpenMetadata is a unified metadata platform. Prior to 1.11.8, calls issued by the UI against /api/v1/ingestionPipelines leak JWTs used by ingestion-bot for certain services (Glue / Redshift / Postgres). Any read-only user can gain access to a highly privileged account, typically which has the Ingestion Bot Role. This enables destructive changes in OpenMetadata instances, and potential data leakage (e.g. sample data, or service metadata which would be unavailable per roles/policies). This vulnerability is fixed in 1.11.8.	7.6	More Details
CVE-2020-37212	SpotMSN 2.4.6 contains a denial of service vulnerability in the registration name input field that allows attackers to crash the application. Attackers can generate a 1000-character payload and paste it into the 'Name' field to trigger an application crash.	7.5	More Details
CVE-2020-37211	SpotIM 2.2 contains a denial of service vulnerability that allows attackers to crash the application by inputting a large buffer in the registration name field. Attackers can generate a 1000-character payload and paste it into the 'Name' field to trigger an application crash.	7.5	More Details
CVE-2020-37173	AVideo Platform 8.1 contains an information disclosure vulnerability that allows attackers to enumerate user details through the playlistsFromUser.json.php endpoint. Attackers can retrieve sensitive user information including email, password hash, and administrative status by manipulating the users_id parameter.	7.5	More Details
CVE-2020-37213	TextCrawler Pro 3.1.1 contains a denial of service vulnerability that allows attackers to crash the application by sending an oversized buffer in the license key field. Attackers can generate a 6000-byte payload and paste it into the activation field to trigger an application crash.	7.5	More Details
CVE-2020-37214	Voyager 1.3.0 contains a directory traversal vulnerability that allows attackers to access sensitive system files by manipulating the asset path parameter. Attackers can exploit the path parameter in /admin/voyager-assets to read arbitrary files like /etc/passwd and .env configuration files.	7.5	More Details
CVE-2025-70886	An issue in halo v.2.22.4 and before allows a remote attacker to cause a denial of service via a crafted payload to the public comment submission endpoint	7.5	More Details
CVE-2020-37210	SpotIE 2.9.5 contains a denial of service vulnerability in the registration key input that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the 'Key' field to trigger an application crash.	7.5	More Details
CVE-2020-37195	BlueAuditor 1.7.2.0 contains a denial of service vulnerability in the registration name input field that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the 'Name' field to trigger an application crash.	7.5	More Details
CVE-2020-37104	ASTPP 4.0.1 contains an information disclosure vulnerability that allows unauthenticated attackers to download database backup files by predicting backup filename patterns. Attackers can generate a list of 6-digit PIN combinations and fuzz the backup download URL to exfiltrate sensitive database information from the /database_backup/ directory.	7.5	More Details
CVE-2020-37175	P2PWIFICAM2 for iOS 10.4.1 contains a denial of service vulnerability that allows attackers to crash the application by manipulating the Camera ID input field. Attackers can paste a 257-character buffer into the Camera ID field to trigger an application crash on iOS devices.	7.5	More Details

CVE-2025-67432	A stack overflow in the ZBarcode_Encode function of Monkeybread Software MBS DynaPDF Plugin v21.3.1.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-69807	p2r3 Bareiron commit: 8e4d4020d is vulnerable to Buffer Overflow, which allows unauthenticated remote attackers to cause a denial of service via a packet sent to the server.	7.5	More Details
CVE-2026-25990	Pillow is a Python imaging library. From 10.3.0 to before 12.1.1, n out-of-bounds write may be triggered when loading a specially crafted PSD image. This vulnerability is fixed in 12.1.1.	7.5	More Details
CVE-2024-26480	An issue in Statping-ng v.0.91.0 allows an attacker to obtain sensitive information via a crafted request to the admin parameter.	7.5	More Details
CVE-2024-50617	Vulnerabilities in the File Download and Get File handler components in CIPPlanner CIPAce before 9.17 allow attackers to download unauthorized files. An authenticated user can easily change the file id parameter or pass the physical file path in the URL query string to retrieve the files. (Retrieval is not intended without correct data access configured for documents.)	7.5	More Details
CVE-2024-26477	An issue in Statping-ng v.0.91.0 allows an attacker to obtain sensitive information via a crafted request to the api parameter of the oauth, amazon_sns, export endpoints.	7.5	More Details
CVE-2020-37215	MSN Password Recovery version 1.30 contains a denial of service vulnerability that allows attackers to crash the application by supplying an oversized input in the registration code field. Attackers can generate a 9000-byte buffer of repeated characters and paste it into the 'User Name and Registration Code' field to trigger an application crash.	7.5	More Details
CVE-2020-37178	KeePass Password Safe versions before 2.44 contain a denial of service vulnerability in the help system's HTML handling. Attackers can trigger the vulnerability by dragging and dropping malicious HTML files into the help area, potentially causing application instability or crash.	7.5	More Details
CVE-2020-37177	BOOTP Turbo 2.0 contains a denial of service vulnerability that allows attackers to crash the application by overwriting the Structured Exception Handler (SEH). Attackers can generate a malicious payload of 2196 bytes with specific byte patterns to trigger an application crash and corrupt the SEH chain.	7.5	More Details
CVE-2020-37196	Dnss Domain Name Search Software contains a denial of service vulnerability that allows attackers to crash the application by providing an oversized registration key. Attackers can generate a 1000-character buffer payload and paste it into the registration key field to trigger an application crash.	7.5	More Details
CVE-2020-37197	Dnss Domain Name Search Software contains a denial of service vulnerability that allows attackers to crash the application by overflowing the 'Name' input field. Attackers can generate a 1000-character buffer payload and paste it into the registration name field to trigger an application crash.	7.5	More Details
CVE-2020-37194	Backup Key Recovery 2.2.5 contains a denial of service vulnerability that allows attackers to crash the application by supplying an overly long registration key. Attackers can generate a 1000-character payload file and paste it into the registration key field to trigger an application crash.	7.5	More Details
CVE-2025-46290	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.4, macOS Sonoma 14.8.4. A remote attacker may be able to cause a denial-of-service.	7.5	More Details
CVE-2020-37193	ZIP Password Recovery 2.30 contains a denial of service vulnerability that allows attackers to crash the application by providing maliciously crafted input. Attackers can create a specially prepared text file with specific characters to trigger an application crash when selecting a ZIP file.	7.5	More Details
CVE-2020-37199	NBMonitor 1.6.6.0 contains a denial of service vulnerability in its registration key input that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the 'Key' field to trigger an application crash.	7.5	More Details
CVE-2020-37200	NetShareWatcher 1.5.8.0 contains a buffer overflow vulnerability in the registration key input that allows attackers to crash the application by supplying oversized input. Attackers can generate a 1000-character payload and paste it into the registration key field to trigger an application crash.	7.5	More Details
CVE-2020-37201	NetShareWatcher 1.5.8.0 contains a buffer overflow vulnerability in the registration name input that allows attackers to crash the application. Attackers can generate a 1000-character payload and paste it into the 'Name' field to trigger an application crash.	7.5	More Details
CVE-2020-37202	NetworkSleuth 3.0.0.0 contains a denial of service vulnerability that allows attackers to crash the application by supplying an oversized registration key. Attackers can generate a 1000-character buffer payload and paste it into the registration key field to trigger an application crash.	7.5	More Details
CVE-2020-37203	Office Product Key Finder 1.5.4 contains a denial of service vulnerability that allows attackers to crash the application by manipulating the registration code input. Attackers can create a specially crafted text file and paste it into the 'Name and Key' field to trigger an application crash.	7.5	More Details
CVE-2020-37191	Top Password Software Dialup Password Recovery 1.30 contains a denial of service vulnerability that allows attackers to crash the application by overflowing input fields. Attackers can trigger the vulnerability by inserting a large 5000-character payload into the User Name and Registration Code input fields.	7.5	More Details
CVE-2020-37190	Top Password Firefox Password Recovery 2.8 contains a denial of service vulnerability that allows attackers to crash the application by overflowing input fields. Attackers can trigger the vulnerability by inserting 5000 characters into the User Name or Registration Code input fields.	7.5	More Details

CVE-2020-37189	TaskCanvas 1.4.0 contains a denial of service vulnerability in the registration code input field that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the registration field to trigger an application crash.	7.5	More Details
CVE-2020-37188	SpotOutlook 1.2.6 contains a denial of service vulnerability in the registration name input field that allows attackers to crash the application. Attackers can overwrite the buffer by pasting 1000 'A' characters into the 'Name' field, causing the application to become unresponsive.	7.5	More Details
CVE-2020-37187	SpotDialup 1.6.7 contains a denial of service vulnerability in the registration name input field that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the 'Name' field to trigger an application crash.	7.5	More Details
CVE-2020-37204	RemShutdown 2.9.0.0 contains a denial of service vulnerability in its registration key input that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the registration key field to trigger an application crash.	7.5	More Details
CVE-2026-26029	sf-mcp-server is an implementation of Salesforce MCP server for Claude for Desktop. A command injection vulnerability exists in sf-mcp-server due to unsafe use of child_process.exec when constructing Salesforce CLI commands with user-controlled input. Successful exploitation allows attackers to execute arbitrary shell commands with the privileges of the MCP server process.	7.5	More Details
CVE-2020-37205	RemShutdown 2.9.0.0 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the 'Name' registration field. Attackers can generate a 1000-character buffer payload and paste it into the registration name field to trigger an application crash.	7.5	More Details
CVE-2020-37185	Backup Key Recovery 2.2.5 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the 'Name' input field. Attackers can generate a 1000-character payload and paste it into the registration name field to trigger an application crash.	7.5	More Details
CVE-2020-37182	Redir 3.3 contains a stack overflow vulnerability in the doproxyconnect() function that allows attackers to crash the application by sending oversized input. Attackers can exploit the sprintf() buffer without proper length checking to overwrite memory and cause a segmentation fault, resulting in program termination.	7.5	More Details
CVE-2020-37206	ShareAlarmPro contains a denial of service vulnerability that allows attackers to crash the application by supplying an oversized registration key. Attackers can generate a 1000-character buffer payload to trigger an application crash when pasted into the registration key field.	7.5	More Details
CVE-2020-37207	SpotDialup 1.6.7 contains a denial of service vulnerability in the registration key input field that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the 'Key' field to trigger an application crash.	7.5	More Details
CVE-2020-37180	GTalk Password Finder 2.2.1 contains a denial of service vulnerability that allows attackers to crash the application by supplying an oversized registration key. Attackers can generate a 1000-character payload and paste it into the 'Key' field to trigger an application crash.	7.5	More Details
CVE-2020-37208	SpotFTP 3.0.0.0 contains a buffer overflow vulnerability in the registration key input field that allows attackers to crash the application. Attackers can generate a 1000-character payload and paste it into the 'Key' field to trigger an application crash and denial of service.	7.5	More Details
CVE-2020-37179	APKF Product Key Finder 2.5.8.0 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the 'Name' input field. Attackers can generate a 1000-character payload and paste it into the registration name field to trigger an application crash.	7.5	More Details
CVE-2020-37209	SpotFTP 3.0.0.0 contains a denial of service vulnerability in the registration name input field that allows attackers to crash the application. Attackers can generate a 1000-character buffer payload and paste it into the 'Name' field to trigger an application crash.	7.5	More Details
CVE-2020-37198	Duplicate Cleaner Pro 4.1.3 contains a denial of service vulnerability that allows attackers to crash the application by injecting an oversized buffer into the license key field. Attackers can generate a 6000-byte payload and paste it into the license activation field to trigger an application crash.	7.5	More Details
CVE-2019-25329	FTP Navigator 8.03 contains a denial of service vulnerability that allows attackers to crash the application by overwriting Structured Exception Handler (SEH) with malicious input. Attackers can generate a payload of 4108 'A' characters followed by 4 'B' characters and 40 'C' characters to trigger a program crash when pasted into the custom command input.	7.5	More Details
CVE-2026-20652	The issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26.3, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3, Safari 26.3. A remote attacker may be able to cause a denial-of-service.	7.5	More Details
CVE-2026-2474	Crypt::URandom versions from 0.41 before 0.55 for Perl is vulnerable to a heap buffer overflow in the XS function crypt_urandom_getrandom(). The function does not validate that the length parameter is non-negative. If a negative value (e.g. -1) is supplied, the expression length + 1u causes an integer wraparound, resulting in a zero-byte allocation. The subsequent call to getrandom(data, length, GRND_NONBLOCK) passes the original negative value, which is implicitly converted to a large unsigned value (typically SIZE_MAX). This can result in writes beyond the allocated buffer, leading to heap memory corruption and application crash (denial of service). In common usage, the length argument is typically hardcoded by the caller, which reduces the likelihood of attacker-controlled exploitation. Applications that pass untrusted input to this parameter may be affected.	7.5	More Details
CVE-2019-25339	GHIA CamIP 1.2 for iOS contains a denial of service vulnerability in the password input field that allows attackers to crash the application. Attackers can paste a 33-character buffer of repeated characters into the password field to trigger an application crash on iOS devices.	7.5	More Details
CVE-	SpotAuditor 5.3.2 contains a denial of service vulnerability in its Base64 decryption feature that allows attackers to crash the		More

2019-25340	application by supplying an oversized buffer. Attackers can generate a malformed input file with 2000 repeated characters to trigger an application crash when pasted into the Base64 Encrypted Password field.	7.5	Details
CVE-2019-25341	iNetTools for iOS 8.20 contains a denial of service vulnerability in the Whois feature that allows attackers to crash the application by manipulating input. Attackers can paste a specially crafted 98-character buffer into the Domain Name field to trigger an application crash.	7.5	More Details
CVE-2019-25342	Centova Cast 3.2.12 contains a denial of service vulnerability that allows attackers to overwhelm the system by repeatedly calling the database export API endpoint. Attackers can trigger 100% CPU load by sending multiple concurrent requests to the /api.php endpoint with crafted parameters.	7.5	More Details
CVE-2026-0958	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.4 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an unauthenticated user to cause denial of service through memory or CPU exhaustion by bypassing JSON validation middleware limits.	7.5	More Details
CVE-2026-21878	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to 1.5.0.rc3, a vulnerability has been discovered in BACnet Stack's file writing functionality where there is no validation of user-provided file paths, allowing attackers to write files to arbitrary directories. This affects apps/readfile/main.c and ports/posix/bacfile-posix.c. This vulnerability is fixed in 1.5.0.rc3.	7.5	More Details
CVE-2026-20660	A path handling issue was addressed with improved logic. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3, Safari 26.3. A remote user may be able to write arbitrary files.	7.5	More Details
CVE-2025-57713	A weak authentication vulnerability has been reported to affect File Station 5. The remote attackers can then exploit the vulnerability to gain sensitive information. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5166 and later	7.5	More Details
CVE-2019-25335	PRO-7070 Hazır Profesyonel Web Sitesi version 1.0 contains an authentication bypass vulnerability in the administration panel login page. Attackers can bypass authentication by using '=' 'or' as both username and password to gain unauthorized access to the administrative interface.	7.5	More Details
CVE-2026-1988	The Flexi Product Slider and Grid for WooCommerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.0.5 via the `flexipsg_carousel` shortcode. This is due to the `theme` parameter being directly concatenated into a file path without proper sanitization or validation, allowing directory traversal. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary PHP files on the server via the `theme` parameter granted they can create posts with shortcodes.	7.5	More Details
CVE-2026-2024	The PhotoStack Gallery plugin for WordPress is vulnerable to SQL Injection via the 'postid' parameter in all versions up to, and including, 0.4.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-20650	A denial-of-service issue was addressed with improved validation. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An attacker in a privileged network position may be able to perform denial-of-service attack using crafted Bluetooth packets.	7.5	More Details
CVE-2025-70956	A State Pollution vulnerability was discovered in the TON Virtual Machine (TVM) before v2025.04. The issue exists in the RUNVM instruction logic (VmState::run_child_vm), which is responsible for initializing child virtual machines. The operation moves critical resources (specifically libraries and log) from the parent state to a new child state in a non-atomic manner. If an Out-of-Gas (OOG) exception occurs after resources are moved but before the state transition is finalized, the parent VM retains a corrupted state where these resources are emptied/invalid. Because RUNVM supports gas isolation, the parent VM continues execution with this corrupted state, leading to unexpected behavior or denial of service within the contract's context.	7.5	More Details
CVE-2026-25949	Traefik is an HTTP reverse proxy and load balancer. Prior to 3.6.8, there is a potential vulnerability in Traefik managing STARTTLS requests. An unauthenticated client can bypass Traefik entrypoint respondingTimeouts.readTimeout by sending the 8-byte Postgres SSLRequest (STARTTLS) prelude and then stalling, causing connections to remain open indefinitely, leading to a denial of service. This vulnerability is fixed in 3.6.8.	7.5	More Details
CVE-2025-70121	An array index out of bounds vulnerability in the AMF component of free5GC v4.0.1 allows remote attackers to cause a denial of service via a crafted 5GS Mobile Identity in a NAS Registration Request message. The issue occurs in the GetSUCI method (NAS_MobileIdentity5GS.go) when accessing index 5 of a 5-element array, leading to a runtime panic and AMF crash.	7.5	More Details
CVE-2025-70122	A heap buffer overflow vulnerability in the UPF component of free5GC v4.0.1 allows remote attackers to cause a denial of service via a crafted PFCP Session Modification Request. The issue occurs in the SDFFilterFields.UnmarshalBinary function (sdf-filter.go) when processing a declared length that exceeds the actual buffer capacity, leading to a runtime panic and UPF crash.	7.5	More Details
CVE-2025-70954	A Null Pointer Dereference vulnerability exists in the TON Virtual Machine (TVM) within the TON Blockchain before v2025.06. The issue is located in the execution logic of the INMSGPARAM instruction, where the program fails to validate if a specific pointer is null before accessing it. By sending a malicious transaction or smart contract, an attacker can trigger this null pointer dereference, causing the validator node process to crash (segmentation fault). This results in a Denial of Service (DoS) affecting the availability of the entire blockchain network.	7.5	More Details
CVE-2019-25338	DokuWiki 2018-04-22b contains a username enumeration vulnerability in its password reset functionality that allows attackers to identify valid user accounts. Attackers can submit different usernames to the password reset endpoint and distinguish between existing and non-existing accounts by analyzing the server's error response messages.	7.5	More Details
CVE-2019-25333	Bullwark Momentum Series JAWS 1.0 contains a directory traversal vulnerability that allows unauthenticated attackers to access system files by manipulating HTTP request paths. Attackers can exploit the vulnerability by sending crafted GET requests with multiple '../' sequences to read sensitive files like /etc/passwd outside the web root directory.	7.5	More Details
CVE-	SurfOffline Professional 2.2.0.103 contains a structured exception handler (SEH) overflow vulnerability that allows attackers to		More

2019-25330	crash the application by manipulating the project name input. Attackers can generate a malicious payload of 382 'A' characters followed by specific byte sequences to trigger a denial of service condition and overwrite SEH registers.	7.5	Details
CVE-2026-2319	Race in DevTools in Google Chrome prior to 145.0.7632.45 allowed a remote attacker who convinced a user to engage in specific UI gestures and install a malicious extension to potentially exploit object corruption via a malicious file. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-20649	A logging issue was addressed with improved data redaction. This issue is fixed in watchOS 26.3, iOS 26.3 and iPadOS 26.3, tvOS 26.3, macOS Tahoe 26.3. A user may be able to view sensitive user information.	7.5	More Details
CVE-2025-69873	ajv (Another JSON Schema Validator) through version 8.17.1 is vulnerable to Regular Expression Denial of Service (ReDoS) when the $data option is enabled. The pattern keyword accepts runtime data via JSON Pointer syntax ($data reference), which is passed directly to the JavaScript RegExp() constructor without validation. An attacker can inject a malicious regex pattern (e.g., "^(a|a)*$") combined with crafted input to cause catastrophic backtracking. A 31-character payload causes approximately 44 seconds of CPU blocking, with each additional character doubling execution time. This enables complete denial of service with a single HTTP request against any API using ajv with $data: true for dynamic schema validation.	7.5	More Details
CVE-2026-26055	Yoke is a Helm-inspired infrastructure-as-code (IaC) package deployer. In 0.19.0 and earlier, a vulnerability exists in the Air Traffic Controller (ATC) component of Yoke. The ATC webhook endpoints lack proper authentication mechanisms, allowing any pod within the cluster network to directly send AdmissionReview requests to the webhook, bypassing Kubernetes API Server authentication. This enables attackers to trigger WASM module execution in the ATC controller context without proper authorization.	7.5	More Details
CVE-2026-0692	The BlueSnap Payment Gateway for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.3.0. This is due to the plugin relying on WooCommerce's `WC_Geolocation::get_ip_address()` function to validate IPN requests, which trusts user-controllable headers like X-Real-IP and X-Forwarded-For to determine the client IP address. This makes it possible for unauthenticated attackers to bypass IP allowlist restrictions by spoofing a whitelisted BlueSnap IP address and send forged IPN (Instant Payment Notification) data to manipulate order statuses (mark orders as paid, failed, refunded, or on-hold) without proper authorization.	7.5	More Details
CVE-2025-70084	Directory traversal vulnerability in OpenSatKit 2.2.1 allows attackers to gain access to sensitive information or delete arbitrary files via crafted value to the FileUtil_GetFileInfo function.	7.5	More Details
CVE-2025-70029	An issue in Sunbird-Ed SunbirdEd-portal v1.13.4 allows attackers to obtain sensitive information. The application disables TLS/SSL certificate validation by setting 'rejectUnauthorized': false in HTTP request options	7.5	More Details
CVE-2019-25322	Heatmiser Netmonitor 3.03 contains a hardcoded credentials vulnerability in the networkSetup.htm page with predictable admin login credentials. Attackers can access the device by using the hard-coded username 'admin' and password 'admin' in the hidden form input fields.	7.5	More Details
CVE-2025-8099	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.8 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions, could have allowed an unauthenticated user to cause denial of service by sending repeated GraphQL queries.	7.5	More Details
CVE-2026-2250	The /dbviewer/ web endpoint in METIS WIC devices is exposed without authentication. A remote attacker can access and export the internal telemetry SQLite database containing sensitive operational data. Additionally, the application is configured with debug mode enabled, causing malformed requests to return verbose Django tracebacks that disclose backend source code, local file paths, and system configuration.	7.5	More Details
CVE-2019-25328	XnConvert 1.82 contains a denial of service vulnerability in its registration code input field that allows attackers to crash the application. Attackers can generate a 9000-byte buffer of repeated characters and paste it into the registration code field to trigger an application crash.	7.5	More Details
CVE-2026-26235	JUNG Smart Visu Server 1.1.1050 contains a denial of service vulnerability that allows unauthenticated attackers to remotely shutdown or reboot the server. Attackers can send a single POST request to trigger the server reboot without requiring any authentication.	7.5	More Details
CVE-2025-70123	An improper input validation and protocol compliance vulnerability in free5GC v4.0.1 allows remote attackers to cause a denial of service. The UPF incorrectly accepts a malformed PFCP Association Setup Request, violating 3GPP TS 29.244. This places the UPF in an inconsistent state where a subsequent valid PFCP Session Establishment Request triggers a cascading failure, disrupting the SMF connection and causing service degradation.	7.5	More Details
CVE-2025-33088	IBM Concert 1.0.0 through 2.1.0 could allow a local user with specific knowledge about the system's architecture to escalate their privileges due to incorrect file permissions for critical resources.	7.4	More Details
CVE-2025-70093	An issue in OpenSourcePOS v3.4.1 allows attackers to execute arbitrary code via returning a crafted AJAX response.	7.4	More Details
CVE-2026-26214	Galaxy FDS Android SDK (XiaoMi/galaxy-fds-sdk-android) version 3.0.8 and prior disable TLS hostname verification when HTTPS is enabled (the default configuration). In GalaxyFDSClientImpl.createHttpClient(), the SDK configures Apache HttpClient with SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER, which accepts any valid TLS certificate regardless of hostname mismatch. Because HTTPS is enabled by default in FDSClientConfiguration, all applications using the SDK with default settings are affected. This vulnerability allows a man-in-the-middle attacker to intercept and modify SDK communications to Xiaomi FDS cloud storage endpoints, potentially exposing authentication credentials, file contents, and API responses. The XiaoMi/galaxy-fds-sdk-android open source project has reached end-of-life status.	7.4	More Details
CVE-	A DLL hijacking vulnerability in Doc Nav could allow a local attacker to achieve privilege escalation, potentially resulting in		More

2025-54519	arbitrary code execution.	7.3	Details
CVE-2026-2549	A vulnerability has been found in zhanghuanhao LibrarySystem 图书馆管理系统 up to 1.1.1. This impacts an unknown function of the file BookController.java. The manipulation leads to improper access controls. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-2621	A security vulnerability has been detected in Sciyon Koyuan Thermoelectricity Heat Network Management System 3.0. This affects an unknown part of the file /SISReport/WebReport20/Proxy/AsyncTreeProxy.aspx. The manipulation of the argument PGUID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-0595	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.9 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an authenticated user to add unauthorized email addresses to victim accounts through HTML injection in test case titles.	7.3	More Details
CVE-2025-14560	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.1 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an authenticated user to perform unauthorized actions on behalf of another user by injecting malicious content into vulnerability code flow.	7.3	More Details
CVE-2026-2544	A security flaw has been discovered in yued-fe LuLu UI up to 3.0.0. This issue affects the function child_process.exec of the file run.js. The manipulation results in os command injection. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-2533	A flaw has been found in Tosei Self-service Washing Machine 4.02. Impacted is an unknown function of the file /cgi-bin/tosei_datasend.php. Executing a manipulation of the argument adr_txt_1 can lead to command 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.	7.3	More Details
CVE-2025-33042	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache Avro Java SDK when generating specific records from untrusted Avro schemas. This issue affects Apache Avro Java SDK: all versions through 1.11.4 and version 1.12.0. Users are recommended to upgrade to version 1.12.1 or 1.11.5, which fix the issue.	7.3	More Details
CVE-2025-40905	WWW::OAuth 1.000 and earlier for Perl uses the rand() function as the default source of entropy, which is not cryptographically secure, for cryptographic functions.	7.3	More Details
CVE-2025-52541	A DLL hijacking vulnerability in Vivado could allow a local attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	7.3	More Details
CVE-2026-2620	A weakness has been identified in Huace Monitoring and Early Warning System 2.2. Affected by this issue is some unknown functionality of the file /Web/SysManage/ProjectRole.aspx. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-2629	A weakness has been identified in jishi node-sonos-http-api up to 3776f0ee2261c924c7b7204de121a38100a08ca7. Affected is the function Promise of the file lib/tts-providers/mac-os.js of the component TTS Provider. This manipulation of the argument phrase causes os command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2023-31313	An unintended proxy or intermediary in the AMD power management firmware (PMFW) could allow a privileged attacker to send malformed messages to the system management unit (SMU) potentially resulting in arbitrary code execution.	7.2	More Details
CVE-2026-1841	The PixelYourSite – Your smart PIXEL (TAG) & API Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pysTrafficSource' parameter and the 'pys_landing_page' parameter in all versions up to, and including, 11.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-1843	The Super Page Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Activity Log in all versions up to, and including, 5.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-15440	The iONE360 configurator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Contact Form Parameters in all versions up to, and including, 2.0.57 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-2026-1844	The PixelYourSite PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pysTrafficSource' parameter and the 'pys_landing_page' parameter in all versions up to, and including, 12.4.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-2567	A vulnerability was detected in Wavlink WL-NU516U1 20251208. This vulnerability affects the function sub_401218 of the file /cgi-bin/nas.cgi. Performing a manipulation of the argument User1Passwd results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	7.2	More Details
CVE-2026-	SmarterTools SmarterMail before 9526 allows XSS via MAPI requests.	7.2	More Details

26930			
CVE-2019-25379	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains stored and reflected cross-site scripting vulnerabilities in the urlfilter.cgi endpoint that allow attackers to inject malicious scripts. Attackers can submit POST requests with script payloads in the REDIRECT_PAGE or CHILDREN parameters to execute arbitrary JavaScript in user browsers.	7.2	More Details
CVE-2019-25394	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple stored cross-site scripting vulnerabilities in the modem.cgi script that allow attackers to inject malicious scripts through POST parameters. Attackers can submit crafted payloads in parameters like INIT, HANGUP, SPEAKER_ON, SPEAKER_OFF, TONE_DIAL, and PULSE_DIAL to execute arbitrary JavaScript in users' browsers when the stored data is retrieved.	7.2	More Details
CVE-2019-25395	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple stored cross-site scripting vulnerabilities in the preferences.cgi script that allow attackers to inject malicious scripts through the HOSTNAME, KEYMAP, and OPENNESS parameters. Attackers can submit POST requests with script payloads to preferences.cgi to store malicious code that executes in the browsers of users accessing the preferences page.	7.2	More Details
CVE-2026-2566	A security vulnerability has been detected in Wavlink WL-NU516U1 up to 130/260. This affects the function sub_406194 of the file /cgi-bin/adm.cgi. Such manipulation of the argument firmware_url leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2026-0753	The Super Simple Contact Form plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'sscf_name' parameter in all versions up to, and including, 1.6.2 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.	7.2	More Details
CVE-2026-1216	The RSS Aggregator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'template' parameter in all versions up to, and including, 5.0.10 due to insufficient input sanitization and output escaping on user supplied attributes. 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.	7.2	More Details
CVE-2026-2615	A flaw has been found in Wavlink WL-NU516U1 up to 20251208. The affected element is the function singlePortForwardDelete of the file /cgi-bin/firewall.cgi. Executing a manipulation of the argument del_flag can lead to command injection. The attack may be launched 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-2026-1320	The Secure Copy Content Protection and Content Locking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'X-Forwarded-For' HTTP header in all versions up to, and including, 4.9.8 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-2026-1316	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'media[].href' parameter in all versions up to, and including, 5.97.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers (if 'Enable for Guests' is enabled) to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-14541	The Lucky Wheel Giveaway plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.0.22 via the conditional_tags parameter. This is due to the plugin using PHP's eval() function on user-controlled input without proper validation or sanitization. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.	7.2	More Details
CVE-2026-0745	The User Language Switch plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.6.10 due to missing URL validation on the 'download_language()' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.2	More Details
CVE-2026-20611	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	7.1	More Details
CVE-2026-20606	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, iOS 26.3 and iPadOS 26.3. An app may be able to bypass certain Privacy preferences.	7.1	More Details
CVE-2026-20641	A privacy issue was addressed with improved checks. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to identify what other apps a user has installed.	7.1	More Details
CVE-2026-25999	Klaw is a self-service Apache Kafka Topic Management/Governance tool/portal. Prior to 2.10.2, there is an improper access control vulnerability that allows unauthorized users to trigger a reset or deletion of metadata for any tenant. By sending a crafted request to the /resetMemoryCache endpoint, an attacker can clear cached configurations, environments, and cluster data. This vulnerability is fixed in 2.10.2.	7.1	More Details
CVE-2025-36247	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.3 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	7.1	More Details
CVE-2026-20628	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to break out of its sandbox.	7.1	More Details
CVE-2019-	thesystem App 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating the username parameter. Attackers can inject malicious SQL code like ' or '1=1 to the username field to gain unauthorized access	7.1	More

25347	to user accounts.		Details
CVE-2019-25346	TheSystem 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating the 'server_name' parameter. Attackers can inject malicious SQL code like ' or '1=1 to retrieve unauthorized database records and potentially access sensitive system information.	7.1	More Details
CVE-2026-26157	A flaw was found in BusyBox. Incomplete path sanitization in its archive extraction utilities allows an attacker to craft malicious archives that when extracted, and under specific conditions, may write to files outside the intended directory. This can lead to arbitrary file overwrite, potentially enabling code execution through the modification of sensitive system files.	7.0	More Details
CVE-2026-20617	A race condition was addressed with improved state handling. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to gain root privileges.	7.0	More Details
CVE-2026-26158	A flaw was found in BusyBox. This vulnerability allows an attacker to modify files outside of the intended extraction directory by crafting a malicious tar archive containing unvalidated hardlink or symlink entries. If the tar archive is extracted with elevated privileges, this flaw can lead to privilege escalation, enabling an attacker to gain unauthorized access to critical system files.	7.0	More Details
CVE-2026-25087	Use After Free vulnerability in Apache Arrow C++. This issue affects Apache Arrow C++ from 15.0.0 through 23.0.0. It can be triggered when reading an Arrow IPC file (but not an IPC stream) with pre-buffering enabled, if the IPC file contains data with variadic buffers (such as Binary View and String View data). Depending on the number of variadic buffers in a record batch column and on the temporal sequence of multi-threaded IO, a write to a dangling pointer could occur. The value (a `std::shared_ptr<Buffer>` object) that is written to the dangling pointer is not under direct control of the attacker. Pre-buffering is disabled by default but can be enabled using a specific C++ API call (`RecordBatchFileReader::PreBufferMetadata`). The functionality is not exposed in language bindings (Python, Ruby, C GLib), so these bindings are not vulnerable. The most likely consequence of this issue would be random crashes or memory corruption when reading specific kinds of IPC files. If the application allows ingesting IPC files from untrusted sources, this could plausibly be exploited for denial of service. Inducing more targeted kinds of misbehavior (such as confidential data extraction from the running process) depends on memory allocation and multi-threaded IO temporal patterns that are unlikely to be easily controlled by an attacker. Advice for users of Arrow C++: 1. check whether you enable pre-buffering on the IPC file reader (using `RecordBatchFileReader::PreBufferMetadata`) 2. if so, either disable pre-buffering (which may have adverse performance consequences), or switch to Arrow 23.0.1 which is not vulnerable	7.0	More Details
CVE-2026-2516	A vulnerability was identified in Unidocs ezPDF DRM Reader and ezPDF Reader 2.0/3.0.0.4 on 32-bit. This affects an unknown part in the library SHFOLDER.dll. Such manipulation leads to uncontrolled search path. The attack needs to be performed locally. Attacks of this nature are highly complex. It is indicated that the exploitability is difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-2542	A weakness has been identified in Total VPN 0.5.29.0 on Windows. Affected by this vulnerability is an unknown functionality of the file C:\Program Files\Total VPN\win-service.exe. Executing a manipulation can lead to unquoted search path. It is possible to launch the attack on the local host. This attack is characterized by high complexity. The exploitation appears to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2026-2538	A security flaw has been discovered in Flos Freeware Notepad2 4.2.22/4.2.23/4.2.24/4.2.25. Affected is an unknown function in the library Msimg32.dll. Performing a manipulation results in uncontrolled search path. Attacking locally is a requirement. The attack's complexity is rated as high. The exploitability is told to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	7.0	More Details
CVE-2025-32063	There is a misconfiguration vulnerability inside the Infotainment ECU manufactured by BOSCH. The vulnerability happens during the startup phase of a specific systemd service, and as a result, the following developer features will be activated: the disabled firewall and the launched SSH server. First identified on Nissan Leaf ZE1 manufactured in 2020.	6.8	More Details
CVE-2025-41117	Stack traces in Grafana's Explore Traces view can be rendered as raw HTML, and thus inject malicious JavaScript in the browser. This would require malicious JavaScript to be entered into the stack trace field. Only datasources with the Jaeger HTTP API appear to be affected; Jaeger gRPC and Tempo do not appear affected whatsoever.	6.8	More Details
CVE-2025-27900	IBM DB2 Recovery Expert for LUW 5.5 Interim Fix 002 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	6.8	More Details
CVE-2026-25933	Arduino App Lab is a cross-platform IDE for developing Arduino Apps. Prior to 0.4.0, a vulnerability was identified in the Terminal component of the arduino-app-lab application. The issue stems from insufficient sanitization and validation of input data received from connected hardware devices, specifically in the _info.Serial and _info.Address metadata fields. The problem occurs during device information handling. When a board is connected, the application collects identifying attributes to establish a terminal session. Because strict validation is not enforced for the Serial and Address parameters, an attacker with control over the connected hardware can supply specially crafted strings containing shell metacharacters. The exploitation requires direct physical access to a previously tampered board. When the host system processes these fields, any injected payload is executed with the privileges of the user running arduino-app-lab. This vulnerability is fixed in 0.4.0.	6.8	More Details
CVE-2025-32060	The system suffers from the absence of a kernel module signature verification. If an attacker can execute commands on behalf of root user (due to additional vulnerabilities), then he/she is also able to load custom kernel modules to the kernel space and execute code in the kernel context. Such a flaw can lead to taking control over the entire system. First identified on Nissan Leaf ZE1 manufactured in 2020.	6.7	More Details
CVE-2026-22284	Dell SmartFabric OS10 Software, versions prior to 10.5.6.12, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	6.6	More Details
CVE-	A weakness has been identified in Wavlink WL-NU516U1 20251208. Affected by this issue is the function sub_40785C of the file /cgi-bin/adm.cgi. This manipulation of the argument time_zone causes stack-based buffer overflow. The attack can be initiated		More

2026-2565	remotely. The attack is considered to have high complexity. The exploitation is known to be difficult. 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.	6.6	Details
CVE-2025-33089	IBM Concert 1.0.0 through 2.1.0 could allow a remote attacker to obtain sensitive information or perform unauthorized actions due to the use of hard coded user credentials.	6.5	More Details
CVE-2025-27904	IBM DB2 Recovery Expert for LUW 5.5 Interim Fix 002 IBM Db2 Recovery Expert for Linux, UNIX and Windows is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	6.5	More Details
CVE-2026-1793	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to arbitrary file reads in all versions up to, and including, 8.3.17 via the SVG widget and a lack of sufficient file validation in the 'render_svg' function. 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-2026-26367	eNet SMART HOME server 2.2.1 and 2.3.1 contains a missing authorization vulnerability in the deleteUserAccount JSON-RPC method that permits any authenticated low-privileged user (UG_USER) to delete arbitrary user accounts, except for the built-in admin account. The application does not enforce role-based access control on this function, allowing a standard user to submit a crafted POST request to /jsonrpc/management specifying another username to have that account removed without elevated permissions or additional confirmation.	6.5	More Details
CVE-2025-13431	The SlimStat Analytics plugin for WordPress is vulnerable to time-based SQL Injection via the ‘args’ parameter in all versions up to, and including, 5.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-70094	A cross-site scripting (XSS) vulnerability in the Generate Item Barcode function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Item Category parameter.	6.5	More Details
CVE-2025-70091	A cross-site scripting (XSS) vulnerability in the Customers function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Phone Number parameter.	6.5	More Details
CVE-2025-8303	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EKA Software Computer Information Advertising Services Ltd. Real Estate Script V5 (With Doping Module – Store Module – New Language System) allows Cross-Site Scripting (XSS).This issue affects Real Estate Script V5 (With Doping Module – Store Module – New Language System): through 17022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2022-41650	Missing Authorization vulnerability in Paul Custom Content by Country (by Shield Security) custom-content-by-country.This issue affects Custom Content by Country (by Shield Security): from n/a through 3.1.2.	6.5	More Details
CVE-2026-20680	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, iOS 26.3 and iPadOS 26.3. A sandboxed app may be able to access sensitive user data.	6.5	More Details
CVE-2024-31118	Missing Authorization vulnerability in Smartypants SP Project & Document Manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SP Project & Document Manager: from n/a through 4.70.	6.5	More Details
CVE-2019-25320	E Learning Script 1.0 contains an authentication bypass vulnerability that allows attackers to access the dashboard without valid credentials by manipulating login parameters. Attackers can exploit the /login.php file by sending a specific payload '=''or' to bypass authentication and gain unauthorized access to the system.	6.5	More Details
CVE-2025-33124	IBM DB2 Merge Backup for Linux, UNIX and Windows 12.1.0.0 could allow an authenticated user to cause the program to crash due to the incorrect calculation of a buffer size.	6.5	More Details
CVE-2025-13867	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.3 could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic	6.5	More Details
CVE-2025-14689	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 12.1.0 through 12.1.3 could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic with federated objects.	6.5	More Details
CVE-2025-36018	IBM Concert 1.0.0 through 2.1.0 for Z hub component is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	6.5	More Details
CVE-2025-56647	npm @farmfe/core before 1.7.6 is Missing Origin Validation in WebSocket. The development (hot module reloading) server does not validate origin when connecting to a WebSocket client. This allows attackers to surveil developers running Farm who visit their webpage and steal source code that is leaked by the WebSocket server.	6.5	More Details
CVE-2026-1671	The Activity Log for WordPress plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the winter_activity_log_action() function in all versions up to, and including, 1.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view potentially sensitive information (e.g., the password of a higher level user, such as an administrator) contained in the exposed log files.	6.5	More Details

CVE-2025-15574	When connecting to the Solax Cloud MQTT server the username is the "registration number", which is the 10 character string printed on the SolaX Power Pocket device / the QR code on the device. The password is derived from the "registration number" using a proprietary XOR/transposition algorithm. Attackers with the knowledge of the registration numbers can connect to the MQTT server and impersonate the dongle / inverters.	6.5	More Details
CVE-2025-27901	IBM DB2 Recovery Expert for LUW 5.5 Interim Fix 002 IBM Db2 Recovery Expert for Linux, UNIX and Windows is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	6.5	More Details
CVE-2026-20644	The issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26.3, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3, Safari 26.3. Processing maliciously crafted web content may lead to an unexpected process crash.	6.5	More Details
CVE-2025-70095	A cross-site scripting (XSS) vulnerability in the item management and sales invoice function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	6.5	More Details
CVE-2026-1387	GitLab has remediated an issue in GitLab EE affecting all versions from 15.6 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an authenticated user to cause Denial of Service by uploading a malicious file and repeatedly querying it through GraphQl.	6.5	More Details
CVE-2025-48722	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2026-2318	Inappropriate implementation in PictureInPicture in Google Chrome prior to 145.0.7632.45 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-2320	Inappropriate implementation in File input in Google Chrome prior to 145.0.7632.45 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2025-54147	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2020-37156	BloodX 1.0 contains an authentication bypass vulnerability in login.php that allows attackers to access the dashboard without valid credentials. Attackers can exploit the vulnerability by sending a crafted payload with '=''or' parameters to bypass login authentication and gain unauthorized access.	6.5	More Details
CVE-2025-54146	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2025-53598	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2025-47209	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2026-2316	Insufficient policy enforcement in Frames in Google Chrome prior to 145.0.7632.45 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2025-36598	Dell Avamar, versions prior to 19.12 with patch 338905, contains an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Security. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to upload malicious files.	6.5	More Details
CVE-2025-30266	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2026-1458	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.0 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an unauthenticated user to cause denial of service by uploading malicious files.	6.5	More Details
CVE-2026-1456	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an unauthenticated user to cause denial of service through CPU exhaustion by submitting specially crafted markdown files that trigger exponential processing in markdown preview.	6.5	More Details
CVE-2026-26012	vaultwarden is an unofficial Bitwarden compatible server written in Rust, formerly known as bitwarden_rs. Prior to 1.35.3, a regular organization member can retrieve all ciphers within an organization, regardless of collection permissions. The endpoint /ciphers/organization-details is accessible to any organization member and internally uses Cipher::find_by_org to retrieve all ciphers. These ciphers are returned with CipherSyncType::Organization without enforcing collection-level access control. This vulnerability is fixed in 1.35.3.	6.5	More Details
CVE-2025-33130	IBM DB2 Merge Backup for Linux, UNIX and Windows 12.1.0.0 could allow an authenticated user to cause the program to crash due to a buffer being overwritten when it is allocated on the stack.	6.5	More Details

CVE-2026-2317	Inappropriate implementation in Animation in Google Chrome prior to 145.0.7632.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2025-54148	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2026-20616	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 18.7.5 and iPadOS 18.7.5, macOS Tahoe 26.3, macOS Sonoma 14.8.4, visionOS 26.3. Processing a maliciously crafted USD file may lead to unexpected app termination.	6.5	More Details
CVE-2026-23596	A vulnerability in the management API of the affected product could allow an unauthenticated remote attacker to trigger service restarts. Successful exploitation could allow an attacker to disrupt services and negatively impact system availability.	6.5	More Details
CVE-2025-62853	A path traversal vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5166 and later	6.5	More Details
CVE-2025-66278	A path traversal vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5190 and later	6.5	More Details
CVE-2025-68406	A path traversal vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2026-22894	A path traversal vulnerability has been reported to affect File Station 6. If a remote attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5190 and later	6.5	More Details
CVE-2026-23598	Vulnerabilities in the API error handling of an HPE Aruba Networking 5G Core server API could allow an unauthenticated remote attacker to obtain sensitive information. Successful exploitation could allow an attacker to access details such as user accounts, roles, and system configuration, as well as to gain insight into internal services and workflows, increasing the risk of unauthorized access and elevated privileges when combined with other vulnerabilities.	6.5	More Details
CVE-2026-23597	Vulnerabilities in the API error handling of an HPE Aruba Networking 5G Core server API could allow an unauthenticated remote attacker to obtain sensitive information. Successful exploitation could allow an attacker to access details such as user accounts, roles, and system configuration, as well as to gain insight into internal services and workflows, increasing the risk of unauthorized access and elevated privileges when combined with other vulnerabilities.	6.5	More Details
CVE-2025-58470	A path traversal vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2025-65127	A lack of session validation in the web API component of Shenzhen Zhibotong Electronics ZBT WE2001 23.09.27 allows remote unauthenticated attackers to access administrative information-retrieval functions intended for authenticated users. By invoking "get_*" operations, attackers can obtain device configuration data, including plaintext credentials, without authentication or an existing session.	6.5	More Details
CVE-2025-58467	A relative path traversal vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2025-57708	An allocation of resources without limits or throttling vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2025-54170	An out-of-bounds read vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2025-54169	An out-of-bounds read vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5068 and later	6.5	More Details
CVE-2026-22762	Dell Avamar Server and Avamar Virtual Edition, versions prior to 19.10 SP1 with CHF338912, contain an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Security. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary file delete.	6.5	More Details
CVE-2025-54152	A use of out-of-range pointer offset vulnerability has been reported to affect Qsync Central. If a remote attacker gains a user account, they can then exploit the vulnerability to read sensitive portions of memory. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	6.5	More Details
CVE-2026-1786	The Twitter posts to Blog plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'dg_tw_options' function in all versions up to, and including, 1.11.25. This makes it possible for unauthenticated attackers to update plugin settings including Twitter API credentials, post author, post status, and the capability required to access the plugin's admin menu.	6.5	More Details
CVE-	An uncontrolled resource consumption vulnerability has been reported to affect File Station 5. If a remote attacker gains a user		More

2025-62854	account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5190 and later	6.5	Details
CVE-2026-20636	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.3 and iPadOS 26.3, Safari 26.3, macOS Tahoe 26.3, visionOS 26.3. Processing maliciously crafted web content may lead to an unexpected process crash.	6.5	More Details
CVE-2025-15400	The Pix para Woocommerce WordPress plugin through 2.13.3 allows any authenticated user to trigger AJAX actions that reset payment gateway configuration options without capability or nonce checks. This permits any authenticated users, such as subscribers to clear API credentials and webhook status, causing persistent disruption of OpenPix payment functionality.	6.5	More Details
CVE-2026-1235	The WP eCommerce WordPress plugin through 3.15.1 unserializes user input via ajax actions, which could allow unauthenticated users to perform PHP Object Injection when a suitable gadget is present on the blog.	6.5	More Details
CVE-2026-1912	The Citations tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'code' parameter in the 'ctdoi' shortcode in all versions up to, and including, 0.3.2 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-2026-0550	The myCred plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mycred_load_coupon' shortcode in all versions up to, and including, 2.9.7.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0736	The Chatbot for WordPress by Collect.chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_inpost_head_script[synth_header_script]' post meta field in all versions up to, and including, 2.4.8 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-2026-0751	The Payment Page | Payment Form for Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pricing_plan_select_text_font_family' parameter in all versions up to, and including, 1.4.6 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-2026-1096	The Best-wp-google-map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'latitude' and 'longitudinal' parameters of the 'google_map_view' shortcode in all versions up to, and including, 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-2026-1187	The ZoomifyWP Free plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'filename' parameter of the 'zoomify' 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-2026-1901	The QuestionPro Surveys plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'questionpro' 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-2026-1903	The Ravelry Designs Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'layout' attribute of the 'sb_ravelry_designs' shortcode in all versions up to, and including, 1.0.0. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1905	The Sphere Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter in the 'show_sphere_image' shortcode 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
CVE-2026-1904	The Simple Wp colorfull Accordion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in the 'accordion' 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-2026-1915	The Simple Plyr plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'poster' parameter in the 'plyr' shortcode in all versions up to, and including, 0.0.1 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-2026-1939	The Percent to Infograph plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `percent_to_graph` 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-2026-1985	The Press3D plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 3D Model Gutenberg block in all versions up to, and including, 1.0.2. This is due to the plugin failing to sanitize and validate the URL scheme when storing link URLs for 3D model blocks, allowing `javascript:` URLs. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages via the link URL parameter that will execute whenever a user clicks on the 3D model.	6.4	More Details
	The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored		

CVE-2026-1512	Cross-Site Scripting via the plugin's Info Box widget in all versions up to, and including, 6.5.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1853	The BuddyHolis ListSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'listsearch' 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-2019-25373	OPNsense 19.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the category parameter. Attackers can send POST requests to firewall_rules_edit.php with script payloads in the category field to execute arbitrary JavaScript in the browsers of other users accessing firewall rule pages.	6.4	More Details
CVE-2019-25317	Kimai 2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into timesheet descriptions. Attackers can insert SVG-based XSS payloads in the description field to execute arbitrary JavaScript when the page is loaded and viewed by other users.	6.4	More Details
CVE-2019-25316	GOautodial 4.0 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the event title parameter. Attackers can exploit the CreateEvent.php endpoint by sending crafted POST requests with XSS payloads to execute arbitrary JavaScript in victim browsers.	6.4	More Details
CVE-2019-25315	WordPress Server Log Viewer 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through unfiltered log file paths. Attackers can add log files with embedded XSS payloads that will execute when viewed in the WordPress admin interface.	6.4	More Details
CVE-2019-25312	InoERP 0.7.2 contains a persistent cross-site scripting vulnerability in the comment section that allows unauthenticated attackers to inject malicious scripts. Attackers can submit comments with JavaScript payloads that execute in other users' browsers, potentially stealing cookies and session information.	6.4	More Details
CVE-2019-25311	thesystem version 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through multiple server data input fields. Attackers can submit crafted script payloads in operating_system, system_owner, system_username, system_password, system_description, and server_name parameters to execute arbitrary JavaScript in victim browsers.	6.4	More Details
CVE-2018-25157	Phraseanet 4.0.3 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts through crafted file names during document uploads. Attackers can upload files with embedded SVG scripts that execute in the browser, potentially stealing cookies or redirecting users when the file is viewed.	6.4	More Details
CVE-2019-25369	OPNsense 19.1 contains a stored cross-site scripting vulnerability in the system_advanced_sysctl.php endpoint that allows attackers to inject persistent malicious scripts via the tunable parameter. Attackers can submit POST requests with script payloads that are stored and executed in the context of authenticated user sessions when the page is viewed.	6.4	More Details
CVE-2026-1893	The Orbisius Random Name Generator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'btn_label' parameter in the 'orbisius_random_name_generator' shortcode 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
CVE-2026-1231	The Beaver Builder Page Builder – Drag and Drop Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `js` Global Settings parameter in all versions up to, and including, 2.10.0.5 due to missing capability checks on save_global_settings() function and insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Custom-level access and above who have been granted beaver builder access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1885	The Slideshow Wp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sswpid' attribute of the 'sswp-slide' shortcode in all versions up to, and including, 1.1. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1910	The UpMenu – Online ordering for restaurants plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'lang' attribute of the 'upmenu-menu' shortcode in all versions up to, and including, 3.1. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0557	The WP Data Access plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpda_app' shortcode in all versions up to, and including, 5.5.63 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-2026-1804	The WDES Responsive Popup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wdes-popup-title' shortcode in all versions up to, and including, 1.3.6 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-2026-1809	The HTML Tag Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes 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-	The OpenPOS Lite – Point of Sale for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter of the order_qrcode shortcode in all versions up to, and including, 3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject	6.4	More Details

1826	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-1827	The Flask Micro code-editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's codeflask 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-2026-0559	The MasterStudy LMS WordPress Plugin – for Online Courses and Education plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'stm_lms_courses_grid_display' shortcode in all versions up to, and including, 3.7.11 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-2026-1821	The Microtango plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'restkey' parameter of the mt_reservation shortcode in all versions up to, and including, 0.9.29 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-2025-36377	IBM Security QRadar EDR 3.12 through 3.12.23 does not invalidate session after a session expiration which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2026-2534	A vulnerability has been found in Comfast CF-N1 V2 2.6.0.2. The affected element is the function sub_44AC4C of the file /cgi-bin/mbox-config?method=SET&section=ptest_bandwidth. The manipulation of the argument bandwidth leads to command 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-2026-2530	A weakness has been identified in Wavlink WL-WN579A3 up to 20210219. This affects the function AddMac of the file /cgi-bin/wireless.cgi. This manipulation of the argument macAddr causes command injection. The attack is possible to be carried out remotely. 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.	6.3	More Details
CVE-2026-2563	A vulnerability was identified in JingDong JD Cloud Box AX6600 up to 4.5.1.r4533. Affected is the function set_stcreenen_deabled_status/get_status of the file /f/service/controlDevice of the component jdcapp_rpc. The manipulation leads to Remote Privilege Escalation. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2532	A vulnerability was detected in lintsinghua DeepAudit up to 3.0.3. This issue affects some unknown processing of the file backend/app/api/v1/endpoints/embedding_config.py of the component IP Address Handler. Performing a manipulation results in server-side request forgery. It is possible to initiate the attack remotely. Upgrading to version 3.0.4 and 3.1.0 is capable of addressing this issue. The patch is named da853fdd8cbe9d42053b45d83f25708ba29b8b27. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-2535	A vulnerability was found in Comfast CF-N1 V2 2.6.0.2. The impacted element is the function sub_44AB9C of the file /cgi-bin/mbox-config?method=SET&section=ptest_channel. The manipulation of the argument channel results in command injection. 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.	6.3	More Details
CVE-2025-27898	IBM DB2 Recovery Expert for LUW 5.5 Interim Fix 002 does not invalidate session after a timeout which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2025-36376	IBM Security QRadar EDR 3.12 through 3.12.23 does not invalidate session after a session expiration which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2026-2617	A vulnerability was found in Beetel 777VR1 up to 01.00.09. This affects an unknown function of the component Telnet Service/SSH Service. The manipulation results in insecure default initialization of resource. The attack can only be performed from the local network. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2562	A vulnerability was determined in JingDong JD Cloud Box AX6600 up to 4.5.1.r4533. This impacts the function cast_streen of the file /jdcapi of the component jdcweb_rpc. Executing a manipulation of the argument File can lead to Remote Privilege Escalation. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2531	A security vulnerability has been detected in MindsDB up to 25.14.1. This vulnerability affects the function clear_filename of the file mindsdb/utilities/security.py of the component File Upload. Such manipulation leads to server-side request forgery. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The name of the patch is 74d6f0fd4b630218519a700fbee1c05c7fd4b1ed. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-2529	A security flaw has been discovered in Wavlink WL-WN579A3 up to 20210219. Affected by this issue is the function DeleteMac of the file /cgi-bin/wireless.cgi. The manipulation of the argument delete_list results in command injection. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2560	A vulnerability has been found in kalcaddle kodbox up to 1.64.05. The impacted element is the function run of the file plugins/fileThumb/lib/VideoResize.class.php of the component Media File Preview Plugin. Such manipulation of the argument localFile leads to os command injection. The attack can be executed 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
	A vulnerability was determined in opencc JFlow up to 20260129. This affects the function Imp_Done of the file		

CVE-2026-2536	src/main/java/bp/wf/httphandler/WF_Admin_AttrFlow.java of the component Workflow Engine. This manipulation of the argument File causes xml external entity reference. 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-2026-2548	A flaw has been found in WAYOS FBM-220G 24.10.19. This affects the function sub_40F820 of the file rc. Executing a manipulation of the argument upnp_waniface/upnp_ssdp_interval/upnp_max_age can lead to command injection. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2526	A vulnerability was found in Wavlink WL-WN579A3 up to 20210219. This impacts the function multi_ssid of the file /cgi-bin/wireless.cgi. Performing a manipulation of the argument SSID2G2 results in command injection. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2623	A flaw has been found in Blossom up to 1.17.1. This issue affects the function put of the file blossom-backend/common/common-iaas/src/main/java/com/blossom/common/iaas/blos/BLOSManager.java of the component File Upload. This manipulation causes path traversal. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2553	A security flaw has been discovered in tushar-2223 Hotel-Management-System up to bb1f3b3666124b888f1e4bcf51b6fba9fbb01d15. This affects an unknown part of the file /home.php of the component HTTP POST Request Handler. Performing a manipulation of the argument Name/Email results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2556	A security vulnerability has been detected in cskefu up to 8.0.1. This issue affects some unknown processing of the file com/cskefu/cc/controller/resource/MediaController.java of the component Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2527	A vulnerability was determined in Wavlink WL-WN579A3 up to 20210219. Affected is an unknown function of the file /cgi-bin/login.cgi. Executing a manipulation of the argument key can lead to command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-13004	Authorization Bypass Through User-Controlled Key vulnerability in Farktor Software E-Commerce Services Inc. E-Commerce Package allows Manipulating User-Controlled Variables.This issue affects E-Commerce Package: through 27112025.	6.3	More Details
CVE-2026-2528	A vulnerability was identified in Wavlink WL-WN579A3 up to 20210219. Affected by this vulnerability is the function Delete_Mac_list of the file /cgi-bin/wireless.cgi. The manipulation of the argument delete_list leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2558	A flaw has been found in GeekAI up to 4.2.4. The affected element is the function Download of the file api/handler/net_handler.go. This manipulation of the argument url causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2561	A vulnerability was found in JingDong JD Cloud Box AX6600 up to 4.5.1.r4533. This affects the function web_get_ddns_uptime of the file /jdcapi of the component jdcweb_rpc. Performing a manipulation results in Remote Privilege Escalation. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2020-37192	MSN Password Recovery 1.30 contains an XML external entity injection vulnerability that allows attackers to read local system files through crafted XML input. Attackers can exploit the 'Favorites' tab by injecting a malicious XML file that references external entities to retrieve sensitive system configuration information.	6.2	More Details
CVE-2025-66676	An issue in IObit Unlocker v1.3.0.11 allows attackers to cause a Denial of Service (DoS) via a crafted request.	6.2	More Details
CVE-2019-25334	Product Key Explorer 4.2.0.0 contains a denial of service vulnerability that allows local attackers to crash the application by overflowing the registration name input field. Attackers can create a specially crafted text file with repeated characters to trigger a buffer overflow when pasted into the registration name field, causing the application to crash.	6.2	More Details
CVE-2019-25393	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation. Attackers can submit POST requests to the smoothinfo.cgi endpoint with script payloads in the WRAP or SECTIONTITLE parameters to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2026-2026	A vulnerability has been identified where weak file permissions in the Nessus Agent directory on Windows hosts could allow unauthorized access, potentially permitting Denial of Service (DoS) attacks.	6.1	More Details
CVE-2025-33135	IBM Financial Transaction Manager for ACH Services and Check Services for Multi-Platform 3.0.0.0 through 3.0.5.4 Interim Fix 027 IBM Financial Transaction Manager for Check Services v3 (Multiplatforms) is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious		More

2019-25376	scripts by submitting crafted payloads through the ignoreLogACL parameter. Attackers can send POST requests to the proxy endpoint with JavaScript code in the ignoreLogACL parameter to execute arbitrary scripts in users' browsers.	6.1	Details
CVE-2019-25375	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the mailserver parameter. Attackers can send POST requests to the monit interface with JavaScript payloads in the mailserver parameter to execute arbitrary code in users' browsers.	6.1	More Details
CVE-2019-25323	Heatmiser Netmonitor v3.03 contains an HTML injection vulnerability in the outputSetup.htm page that allows attackers to inject malicious HTML code through the outputtitle parameter. Attackers can craft specially formatted POST requests to the outputtitle parameter to execute arbitrary HTML and potentially manipulate the web interface's displayed content.	6.1	More Details
CVE-2019-25324	RICOH Web Image Monitor 1.09 contains an HTML injection vulnerability in the address configuration CGI script that allows attackers to inject malicious HTML code. Attackers can exploit the entryNameIn and entryDisplayNameIn parameters to insert arbitrary HTML content, potentially enabling cross-site scripting attacks.	6.1	More Details
CVE-2019-25374	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by exploiting the passthrough_networks parameter in vpn_ipsec_settings.php. Attackers can craft POST requests with JavaScript payloads in the passthrough_networks parameter to execute arbitrary code in users' browsers.	6.1	More Details
CVE-2019-25372	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation in the host parameter. Attackers can submit crafted payloads through POST requests to diag_traceroute.php to execute arbitrary JavaScript in the context of a user's browser session.	6.1	More Details
CVE-2019-25371	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation in the host parameter. Attackers can submit crafted POST requests to the diag_ping.php endpoint with script payloads in the host parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25370	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input through multiple parameters. Attackers can send POST requests to interfaces_vlan_edit.php with script payloads in the tag, descr, or vlanif parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2026-1164	The Easy Voice Mail plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘message’ parameter in all versions up to, and including, 1.2.5 due to insufficient input sanitization and output escaping. 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.	6.1	More Details
CVE-2026-1754	The personal-authors-category plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL path in all versions up to, and including, 0.3 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-2025-70845	lty628 aidigu v1.9.1 is vulnerable to Cross Site Scripting (XSS) exists in the /setting/ page where the "intro" field is not properly sanitized or escaped.	6.1	More Details
CVE-2019-25385	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the MACHINE and MACHINECOMMENT parameters. Attackers can send POST requests to the outgoing.cgi endpoint with script payloads to execute arbitrary JavaScript in users' browsers and steal session data.	6.1	More Details
CVE-2019-25378	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple cross-site scripting vulnerabilities in the proxy.cgi endpoint that allow attackers to inject malicious scripts through parameters including CACHE_SIZE, MAX_SIZE, MIN_SIZE, MAX_OUTGOING_SIZE, and MAX_INCOMING_SIZE. Attackers can submit POST requests with script payloads to store or reflect arbitrary JavaScript code that executes in users' browsers when the proxy configuration page is accessed.	6.1	More Details
CVE-2019-25386	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the dmzholes.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests with script payloads in the SRC_IP, DEST_IP, or COMMENT parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2026-1792	The Geo Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL path 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 will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2026-1795	The Address Bar Ads plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL Path in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-1796	The StyleBidet plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL path in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-70297	A stored cross-site scripting (XSS) vulnerability in the recipe asset upload and media serving component in Mealie 3.3.1 allows remote authenticated users to inject arbitrary web script or HTML via an uploaded SVG file that is served as image/svg+xml and rendered by a victim s browser.	6.1	More Details
CVE-2019-25380	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the dhcp.cgi script that allow attackers to inject malicious scripts through multiple parameters. Attackers can submit POST requests to dhcp.cgi with script payloads in parameters such as BOOT_SERVER, BOOT_FILE, BOOT_ROOT, START_ADDR, END_ADDR, DNS1, DNS2, NTP1, NTP2, WINS1, WINS2, DEFAULT_LEASE_TIME, MAX_LEASE_TIME, DOMAIN_NAME, NIS_DOMAIN, NIS1, NIS2, STATIC_HOST, STATIC_DESC, STATIC_MAC, and STATIC_IP to execute arbitrary JavaScript in user browsers.	6.1	More Details

CVE-2019-25381	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the hosts.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests to the hosts.cgi endpoint with script payloads in the IP, HOSTNAME, or COMMENT parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2025-36019	IBM Concert 1.0.0 through 2.1.0 for Z hub framework is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2019-25383	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the apcupsd.cgi script that allow attackers to inject malicious scripts through multiple POST parameters. Attackers can submit crafted POST requests with script payloads in parameters like BATTLEVEL, RTMIN, BATTDELAY, TO, ANNOY, UPSIP, UPSNAME, UPSPORT, POLLTIME, UPSUSER, NISPORT, UPSAUTH, EMAIL, FROM, CC, SMSEMAIL, SMTPSERVER, PORT, USER, and EMAIL_PASSWORD to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2019-25384	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the portfw.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests with script payloads in the EXT, SRC_PORT_SEL, SRC_PORT, DEST_IP, DEST_PORT_SEL, or COMMENT parameters to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25382	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the NTP_SERVER parameter. Attackers can send POST requests to the time.cgi endpoint with script payloads in the NTP_SERVER parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25387	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the xtaccess.cgi endpoint. Attackers can inject script payloads through the EXT, DEST_PORT, or COMMENT parameters via POST requests to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2019-25388	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the ipblock.cgi endpoint. Attackers can inject script tags through the SRC_IP and COMMENT parameters in POST requests to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2019-25392	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the IP parameter. Attackers can send POST requests to the iptools.cgi endpoint with script payloads in the IP parameter to execute arbitrary JavaScript in victim browsers.	6.1	More Details
CVE-2019-25389	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the MACHINES parameter. Attackers can craft requests to the timedaccess.cgi endpoint with script payloads in the MACHINES parameter to execute arbitrary JavaScript in users' browsers.	6.1	More Details
CVE-2025-7706	Missing Authentication for Critical Function vulnerability in TUBITAK BILGEM Software Technologies Research Institute Liderahenk allows Remote Code Inclusion.This issue affects Liderahenk: from 3.0.0 to 3.3.1 before 3.5.0.	6.1	More Details
CVE-2026-26023	Dify is an open-source LLM app development platform. Prior to 1.13.0, a cross site scripting vulnerability has been found in the web application chat frontend when using echarts. User or llm inputs containing echarts containing a specific javascript payload will be executed. This vulnerability is fixed in 1.13.0.	6.1	More Details
CVE-2025-48508	Improper Hardware reset flow logic in the GPU GFX Hardware IP block could allow a privileged attacker in a guest virtual machine to control reset operation potentially causing host or GPU crash or reset resulting in denial of service.	6.0	More Details
CVE-2025-46310	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.7.4, macOS Sonoma 14.8.4. An attacker with root privileges may be able to delete protected system files.	6.0	More Details
CVE-2024-43178	IBM Concert 1.0.0 through 2.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details
CVE-2025-36379	IBM Security QRadar EDR 3.12 through 3.12.23 IBM Security ReaQta uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details
CVE-2026-26014	Pion DTLS is a Go implementation of Datagram Transport Layer Security. Pion DTLS versions v1.0.0 through v3.0.10 and 3.1.0 use random nonce generation with AES GCM ciphers, which makes it easier for remote attackers to obtain the authentication key and spoof data by leveraging the reuse of a nonce in a session and a "forbidden attack". Upgrade to v3.0.11, v3.1.1, or later.	5.9	More Details
CVE-2025-27903	IBM DB2 Recovery Expert for LUW 5.5 Interim Fix 002 IBM Db2 Recovery Expert for Linux, UNIX and Windows transmits data in a cleartext communication channel that could allow an attacker to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2025-33101	IBM Concert 1.0.0 through 2.1.0 could allow an attacker to obtain sensitive information using man in the middle techniques due to improper clearing of heap memory.	5.9	More Details
	The Product Options and Price Calculation Formulas for WooCommerce – Uni CPO (Premium) plugin for WordPress is vulnerable		

CVE-2025-13391	to unauthorized loss of data due to a missing capability check on the 'uni_cpo_remove_file' function in all versions up to, and including, 4.9.60. This makes it possible for unauthenticated attackers to delete arbitrary attachments or files stored in Dropbox if the file path is known. The vulnerability was partially patched in version 4.9.60.	5.8	More Details
CVE-2026-0829	The Frontend File Manager Plugin WordPress plugin through 23.5 allows unauthenticated users to send emails through the site without any security checks. This lets attackers use the WordPress site as an open relay for spam or phishing emails to anyone. Attackers can also guess file IDs to access and share uploaded files without permission, exposing sensitive information.	5.8	More Details
CVE-2025-70829	An information exposure vulnerability in Datart v1.0.0-rc.3 allows authenticated attackers to access sensitive data via a custom H2 JDBC connection string.	5.7	More Details
CVE-2025-13821	Mattermost versions 11.1.x <= 11.1.2, 10.11.x <= 10.11.9, 11.2.x <= 11.2.1 fail to sanitize sensitive data in WebSocket messages which allows authenticated users to exfiltrate password hashes and MFA secrets via profile nickname updates or email verification events. Mattermost Advisory ID: MMSA-2025-00560	5.7	More Details
CVE-2025-46300	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Sonoma 14.8.4. A malicious HID device may cause an unexpected process crash.	5.7	More Details
CVE-2025-46303	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Sonoma 14.8.4. A malicious HID device may cause an unexpected process crash.	5.7	More Details
CVE-2025-46302	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Sonoma 14.8.4. A malicious HID device may cause an unexpected process crash.	5.7	More Details
CVE-2025-46304	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Sonoma 14.8.4. A malicious HID device may cause an unexpected process crash.	5.7	More Details
CVE-2025-46305	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Sonoma 14.8.4. A malicious HID device may cause an unexpected process crash.	5.7	More Details
CVE-2025-46301	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Sonoma 14.8.4. A malicious HID device may cause an unexpected process crash.	5.7	More Details
CVE-2024-56807	An out-of-bounds read vulnerability has been reported to affect Media Streaming add-on. If an attacker gains local network access, they can then exploit the vulnerability to obtain secret data. We have already fixed the vulnerability in the following version: Media Streaming add-on 500.1.1.6 (2024/08/02) and later	5.5	More Details
CVE-2025-54151	An uncontrolled resource consumption vulnerability has been reported to affect Qsync Central. If a local attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	5.5	More Details
CVE-2025-54150	An uncontrolled resource consumption vulnerability has been reported to affect Qsync Central. If a local attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	5.5	More Details
CVE-2026-2552	A vulnerability was identified in ZenTao up to 21.7.8. Affected by this issue is the function delete of the file editor/control.php of the component Committer. Such manipulation of the argument filePath leads to path traversal. Upgrading to version 21.7.9 can resolve this issue. The affected component should be upgraded.	5.5	More Details
CVE-2025-54149	An uncontrolled resource consumption vulnerability has been reported to affect Qsync Central. If a local attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	5.5	More Details
CVE-2026-21870	BACnet Protocol Stack library provides a BACnet application layer, network layer and media access (MAC) layer communications services. In 1.4.2, 1.5.0.rc2, and earlier, an off-by-one stack-based buffer overflow in the ubasic interpreter causes a crash (SIGABRT) when processing string literals longer than the buffer limit. The tokenizer_string function in src/bacnet/basic/program/ubasic/tokenizer.c incorrectly handles null termination for maximum-length strings. It writes a null byte to dest[40] when the buffer size is only 40 (indices 0-39), triggering a stack overflow.	5.5	More Details
CVE-2026-20638	A logic issue was addressed with improved checks. This issue is fixed in iOS 26.3 and iPadOS 26.3. A user with Live Caller ID app extensions turned off could have identifying information leaked to the extensions.	5.5	More Details
CVE-2026-20629	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Tahoe 26.3. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2026-20625	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3, macOS Sonoma 14.8.4, visionOS 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20627	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in watchOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to access sensitive user data.	5.5	More Details

CVE-2025-43537	A path handling issue was addressed with improved validation. This issue is fixed in iOS 18.7.5 and iPadOS 18.7.5. Restoring a maliciously crafted backup file may lead to modification of protected system files.	5.5	More Details
CVE-2026-20624	An injection issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3, macOS Sonoma 14.8.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20653	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43417	A path handling issue was addressed with improved logic. This issue is fixed in macOS Sonoma 14.8.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2026-20619	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20621	The issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to cause unexpected system termination or corrupt kernel memory.	5.5	More Details
CVE-2026-20675	The issue was addressed with improved bounds checks. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. Processing a maliciously crafted image may lead to disclosure of user information.	5.5	More Details
CVE-2026-20655	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3, iOS 18.7.5 and iPadOS 18.7.5. An attacker with physical access to a locked device may be able to view sensitive user information.	5.5	More Details
CVE-2025-43403	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.4, macOS Sonoma 14.8.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20647	This issue was addressed with improved data protection. This issue is fixed in macOS Tahoe 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20648	A privacy issue was addressed by moving sensitive data to a protected location. This issue is fixed in macOS Tahoe 26.3. A malicious app may be able to access notifications from other iCloud devices.	5.5	More Details
CVE-2026-25062	Outline is a service that allows for collaborative documentation. Prior to 1.4.0, during the JSON import process, the value of attachments[].key from the imported JSON is passed directly to path.join(rootPath, node.key) and then read using fs.readFile without validation. By embedding path traversal sequences such as ../ or absolute paths, an attacker can read arbitrary files on the server and import them as attachments. This vulnerability is fixed in 1.4.0.	5.5	More Details
CVE-2026-20654	The issue was addressed with improved memory handling. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2026-20634	The issue was addressed with improved memory handling. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2026-20678	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3, iOS 18.7.5 and iPadOS 18.7.5. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20630	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.3. An app may be able to access protected user data.	5.5	More Details
CVE-2026-20666	An authorization issue was addressed with improved state management. This issue is fixed in macOS Tahoe 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20669	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Tahoe 26.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2026-20623	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Tahoe 26.3. An app may be able to access protected user data.	5.5	More Details
CVE-2025-70092	A cross-site scripting (XSS) vulnerability in the Item Kits function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Item Name parameter.	5.5	More Details
CVE-	A privacy issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3, macOS		More

2026-20612	Sonoma 14.8.4. An app may be able to access sensitive user data.	5.5	Details
CVE-2026-20618	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Tahoe 26.3. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2019-25314	Yoast Duplicate-Post WordPress Plugin 3.2.3 contains a persistent cross-site scripting vulnerability in plugin settings parameters. Attackers can inject malicious scripts into title prefix, suffix, menu order, and blacklist fields to execute arbitrary JavaScript in admin interfaces.	5.5	More Details
CVE-2025-13108	IBM DB2 Merge Backup for Linux, UNIX and Windows 12.1.0.0 could allow an attacker to access sensitive information in memory due to the buffer not properly clearing resources.	5.5	More Details
CVE-2026-20602	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3, macOS Sonoma 14.8.4. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2026-20608	This issue was addressed through improved state management. This issue is fixed in macOS Tahoe 26.3, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3, Safari 26.3. Processing maliciously crafted web content may lead to an unexpected process crash.	5.5	More Details
CVE-2024-36316	The integer overflow vulnerability within AMD Graphics driver could allow an attacker to bypass size checks potentially resulting in a denial of service	5.5	More Details
CVE-2026-1987	The Scheduler Widget plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 0.1.6. This is due to the `scheduler_widget_ajax_save_event()` function lacking proper authorization checks and ownership verification when updating events. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify any event in the scheduler via the `id` parameter granted they have knowledge of the event ID.	5.4	More Details
CVE-2026-2322	Inappropriate implementation in File input in Google Chrome prior to 145.0.7632.45 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	5.4	More Details
CVE-2026-0727	The Accordion and Accordion Slider plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.4.5. This is due to the plugin not properly verifying that a user is authorized to perform an action in the 'wp_aas_save_attachment_data' and 'wp_aas_get_attachment_edit_form' functions. This makes it possible for authenticated attackers, with contributor level access and above, to read and modify attachment metadata including file paths, titles, captions, alt text, and custom links for any attachment on the site.	5.4	More Details
CVE-2026-2551	A vulnerability was determined in ZenTao up to 21.7.8. Affected by this vulnerability is the function delete of the file editor/control.php of the component Backup Handler. This manipulation of the argument fileName causes path traversal. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	5.4	More Details
CVE-2026-23861	Dell Unisphere for PowerMax vApp, version(s) 9.2.4.x, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	5.4	More Details
CVE-2019-25377	OPNsense 19.1 contains a reflected cross-site scripting vulnerability in the system_advanced_sysctl.php endpoint that allows attackers to inject malicious scripts via the value parameter. Attackers can craft POST requests with script payloads in the value parameter to execute JavaScript in the context of authenticated user sessions.	5.4	More Details
CVE-2026-0999	Mattermost versions 11.1.x <= 11.1.2, 10.11.x <= 10.11.9, 11.2.x <= 11.2.1 fail to properly validate login method restrictions which allows an authenticated user to bypass SSO-only login requirements via userID-based authentication. Mattermost Advisory ID: MMSA-2025-00548	5.4	More Details
CVE-2019-25368	OPNsense 19.1 contains multiple cross-site scripting vulnerabilities in the diag_backup.php endpoint that allow attackers to inject malicious scripts through multiple parameters including GDrive_GDriveEmail, GDrive_GDriveFolderID, GDrive_GDriveBackupCount, Nextcloud_url, Nextcloud_user, Nextcloud_password, Nextcloud_password_encryption, and Nextcloud_backupdir. Attackers can submit POST requests with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated administrator sessions.	5.4	More Details
CVE-2025-10912	Authorization Bypass Through User-Controlled Key vulnerability in Saastech Cleaning and Internet Services Inc. TemizlikYolda allows Manipulating User-Controlled Variables.This issue affects TemizlikYolda: through 11022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2025-36243	IBM Concert 1.0.0 through 2.1.0 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Details
CVE-2025-12575	GitLab has remediated an issue in GitLab EE affecting all versions from 18.0 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an authenticated user with certain permissions to make unauthorized requests to internal network services through the GitLab server.	5.4	More Details
CVE-2019-25367	ArangoDB Community Edition 3.4.2-1 contains multiple cross-site scripting vulnerabilities in the Aardvark web admin interface (index.html) through search, user management, and API parameters. Attackers can inject scripts via parameters in /_db/_system/_admin/aardvark/index.html to execute JavaScript in authenticated users' browsers.	5.4	More Details
	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the		

CVE-2019-25390	interfaces.cgi script that allow attackers to inject malicious scripts through multiple parameters including GREEN_ADDRESS, GREEN_NETMASK, RED_DHCP_HOSTNAME, RED_ADDRESS, DNS1_OVERRIDE, DNS2_OVERRIDE, RED_MAC, RED_NETMASK, DEFAULT_GATEWAY, DNS1, and DNS2. Attackers can craft POST requests to interfaces.cgi with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated administrator sessions.	5.4	More Details
CVE-2026-26269	Vim is an open source, command line text editor. Prior to 9.1.2148, a stack buffer overflow vulnerability exists in Vim's NetBeans integration when processing the specialKeys command, affecting Vim builds that enable and use the NetBeans feature. The Stack buffer overflow exists in special_keys() (in src/netbeans.c). The while (*tok) loop writes two bytes per iteration into a 64-byte stack buffer (keybuf) with no bounds check. A malicious NetBeans server can overflow keybuf with a single specialKeys command. The issue has been fixed as of Vim patch v9.1.2148.	5.4	More Details
CVE-2025-14289	IBM webMethods Integration Server 12.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	5.4	More Details
CVE-2025-70296	A stored HTML injection vulnerability in the Recipe Notes rendering component in Mealie 3.3.1 allows remote authenticated users to inject arbitrary HTML, resulting in user interface redressing within the recipe view.	5.4	More Details
CVE-2025-14282	A flaw was found in Dropbear. When running in multi-user mode and authenticating users, the dropbear ssh server does the socket forwardings requested by the remote client as root, only switching to the logged-in user upon spawning a shell or performing some operations like reading the user's files. With the recent ability of also using unix domain sockets as the forwarding destination any user able to log in via ssh can connect to any unix socket with the root's credentials, bypassing both file system restrictions and any SO_PEERCRED / SO_PASSCRED checks performed by the peer.	5.4	More Details
CVE-2026-25828	grub-btrfs through 2026-01-31 (on Arch Linux and derivative distributions) allows initramfs OS command injection because it does not sanitize the $root parameter to resolve_device().	5.4	More Details
CVE-2026-26357	Dell Unisphere for PowerMax, version(s) 9.2.4.x, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	5.4	More Details
CVE-2026-26031	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to 2.44.0, security issue was identified in Frappe Learning, where unauthorised users were able to access the full list of enrolled students (by email) in batches. This vulnerability is fixed in 2.44.0.	5.3	More Details
CVE-2026-2524	A flaw has been found in Open5GS 2.7.6. The impacted element is the function mme_s11_handle_create_session_response of the component MME. This manipulation causes denial of service. The attack can be initiated remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-2525	A vulnerability has been found in Free5GC up to 4.1.0. This affects an unknown function of the component PFCP UDP Endpoint. Such manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2026-21722	Public dashboards with annotations enabled did not limit their annotation timerange to the locked timerange of the public dashboard. This means one could read the entire history of annotations visible on the specific dashboard, even those outside the locked timerange. This did not leak any annotations that would not otherwise be visible on the public dashboard.	5.3	More Details
CVE-2026-1833	The WaMate Confirm – Order Confirmation plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 2.0.1. 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 subscriber-level access and above, to block and unblock phone numbers, which should be restricted to administrators.	5.3	More Details
CVE-2023-38265	IBM Cloud Pak System 2.3.3.6, 2.3.3.7, 2.3.4.0, 2.3.4.1, and 2.3.5.0 could disclose folder location information to an unauthenticated attacker that could aid in further attacks against the system.	5.3	More Details
CVE-2026-2295	The WPZOOM Addons for Elementor – Starter Templates & Widgets plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'ajax_post_grid_load_more' function in all versions up to, and including, 1.3.2. This makes it possible for unauthenticated attackers to retrieve protected (draft, future, pending) post titles and excerpts that should not be accessible to unauthenticated users.	5.3	More Details
CVE-2026-20682	A logic issue was addressed with improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3, iOS 18.7.5 and iPadOS 18.7.5. An attacker may be able to discover a user’s deleted notes.	5.3	More Details
CVE-2026-2327	Versions of the package markdown-it from 13.0.0 and before 14.1.1 are vulnerable to Regular Expression Denial of Service (ReDoS) due to the use of the regex /*+$/ in the linkify function. An attacker can supply a long sequence of * characters followed by a non-matching character, which triggers excessive backtracking and may lead to a denial-of-service condition.	5.3	More Details
CVE-2026-1932	The Appointment Booking Calendar Plugin – Bookr plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update-appointment REST API endpoint in all versions up to, and including, 1.0.2. This makes it possible for unauthenticated attackers to modify the status of any appointment.	5.3	More Details
CVE-2026-1537	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the load_step() function in all versions up to, and including, 5.2.6. This makes it possible for unauthenticated attackers to view booking information including customer names, email addresses, phone numbers, appointment times, and service details.	5.3	More Details
CVE-	A weakness has been identified in Open5GS up to 2.7.6. This issue affects the function sgwc_s5c_handle_create_session_response of the component SGW-C. Executing a manipulation can lead to memory corruption.		More

2026-2521	The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.3	Details
CVE-2025-27899	IBM DB2 Recovery Expert for LUW 5.5 Interim Fix 002 discloses sensitive information in an environment variable that could aid in further attacks against the system.	5.3	More Details
CVE-2025-14608	The WP Last Modified Info plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.9.5. This is due to the plugin not validating a user's access to a post before modifying its metadata in the 'bulk_save' AJAX action. This makes it possible for authenticated attackers, with Author-level access and above, to update the last modified metadata and lock the modification date of arbitrary posts, including those created by Administrators via the 'post_ids' parameter.	5.3	More Details
CVE-2026-2522	A security vulnerability has been detected in Open5GS up to 2.7.6. Impacted is an unknown function of the file /src/mme/esm-build.c of the component MME. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2025-14067	The Easy Form Builder plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on multiple AJAX actions in all versions up to, and including, 3.9.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive form response data, including messages, admin replies, and user information due to a logic error in the authorization check that uses AND (&&) instead of OR (||).	5.3	More Details
CVE-2025-13973	The StickEasy Protected Contact Form plugin for WordPress is vulnerable to Sensitive Information Disclosure in all versions up to, and including, 1.0.2. The plugin stores spam detection logs at a predictable publicly accessible location (wp-content/uploads/stickeasy-protected-contact-form/spcf-log.txt). This makes it possible for unauthenticated attackers to download the log file and access sensitive information including visitor IP addresses, email addresses, and comment snippets from contact form submissions that were flagged as spam.	5.3	More Details
CVE-2025-6792	The One to one user Chat by WPGuppy plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the /wp-json/guppylite/v2/channel-authorize rest endpoint in all versions up to, and including, 1.1.4. This makes it possible for unauthenticated attackers to intercept and view private chat messages between users.	5.3	More Details
CVE-2025-15575	The firmware update functionality does not verify the authenticity of the supplied firmware update files. This allows attackers to flash malicious firmware update files on the device. Initial analysis of the firmware update functionality does not show any cryptographic checks (e.g. digital signature checks) on the supplied firmware update files. Furthermore, ESP32 security features such as secure boot are not used.	5.3	More Details
CVE-2025-64074	A path-traversal vulnerability in the logout functionality of Shenzhen Zhibotong Electronics ZBT WE2001 23.09.27 allows remote attackers to delete arbitrary files on the host by supplying a crafted session cookie value.	5.3	More Details
CVE-2026-2523	A vulnerability was detected in Open5GS up to 2.7.6. The affected element is the function smf_gn_handle_create_pdp_context_request of the file /src/smf/gn-handler.c of the component SMF. The manipulation results in reachable assertion. It is possible to launch the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2020-37172	AVideo Platform 8.1 contains a cross-site request forgery vulnerability that allows attackers to reset user passwords by exploiting the password recovery mechanism. Attackers can craft malicious requests to the recoverPass endpoint using the user's recovery token to change account credentials without authentication.	5.3	More Details
CVE-2026-21438	webtransport-go is an implementation of the WebTransport protocol. Prior to 0.10.0, an attacker can cause unbounded memory consumption repeatedly creating and closing many WebTransport streams. Closed streams were not removed from an internal session map, preventing garbage collection of their resources. This vulnerability is fixed in v0.10.0.	5.3	More Details
CVE-2025-36425	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.3 could allow an authenticated user to obtain sensitive information under specific HADR configuration.	5.3	More Details
CVE-2026-2517	A security flaw has been discovered in Open5GS up to 2.7.6. This vulnerability affects the function ogs_gtp2_parse_tft in the library lib/gtp/v2/types.c of the component SMF. Performing a manipulation of the argument pf[0].content.length results in denial of service. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2024-26478	An issue in Statping-ng v.0.91.0 allows an attacker to obtain sensitive information via a crafted request to the /api/users endpoint.	5.3	More Details
CVE-2026-1657	The EventPrime plugin for WordPress is vulnerable to unauthorized image file upload in all versions up to, and including, 4.2.8.4. This is due to the plugin registering the upload_file_media AJAX action as publicly accessible (nopriv-enabled) without implementing any authentication, authorization, or nonce verification despite a nonce being created. This makes it possible for unauthenticated attackers to upload image files to the WordPress uploads directory and create Media Library attachments via the ep_upload_file_media endpoint.	5.3	More Details
CVE-2024-26479	An issue in Statping-ng v.0.91.0 allows an attacker to obtain sensitive information via a crafted request to the Command execution function.	5.3	More Details
CVE-2026-20676	This issue was addressed through improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3, Safari 26.3, macOS Tahoe 26.3, visionOS 26.3. A website may be able to track users through Safari web extensions.	5.3	More Details

CVE-2026-26185	Directus is a real-time API and App dashboard for managing SQL database content. Before 11.14.1, a timing-based user enumeration vulnerability exists in the password reset functionality. When an invalid reset_url parameter is provided, the response time differs by approximately 500ms between existing and non-existing users, enabling reliable user enumeration. This vulnerability is fixed in 11.14.1.	5.3	More Details
CVE-2020-37158	AVideo Platform 8.1 contains a cross-site request forgery vulnerability that allows attackers to reset user passwords by exploiting the password recovery mechanism. Attackers can craft malicious requests to the recoverPass endpoint using the user's recovery token to change account credentials without authentication.	5.3	More Details
CVE-2026-20673	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Tahoe 26.3, macOS Sonoma 14.8.4. Turning off "Load remote content in messages" may not apply to all mail previews.	5.3	More Details
CVE-2026-21435	webtransport-go is an implementation of the WebTransport protocol. Prior to v0.10.0, an attacker can cause a denial of service in webtransport-go by preventing or indefinitely delaying WebTransport session closure. A malicious peer can withhold QUIC flow control credit on the CONNECT stream, blocking transmission of the WT_CLOSE_SESSION capsule and causing the close operation to hang. This vulnerability is fixed in v0.10.0.	5.3	More Details
CVE-2026-21434	webtransport-go is an implementation of the WebTransport protocol. From 0.3.0 to 0.9.0, an attacker can cause excessive memory consumption in webtransport-go's session implementation by sending a WT_CLOSE_SESSION capsule containing an excessively large Application Error Message. The implementation does not enforce the draft-mandated limit of 1024 bytes on this field, allowing a peer to send an arbitrarily large message payload that is fully read and stored in memory. This allows an attacker to consume an arbitrary amount of memory. The attacker must transmit the full payload to achieve the memory consumption, but the lack of any upper bound makes large-scale attacks feasible given sufficient bandwidth. This vulnerability is fixed in 0.10.0.	5.3	More Details
CVE-2026-2443	A flaw was identified in libsoup, a widely used HTTP library in GNOME-based systems. When processing specially crafted HTTP Range headers, the library may improperly validate requested byte ranges. In certain build configurations, this could allow a remote attacker to access portions of server memory beyond the intended response. Exploitation requires a vulnerable configuration and access to a server using the embedded SoupServer component.	5.3	More Details
CVE-2026-1944	The CallbackKiller service widget plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the cbk_save() function in all versions up to, and including, 1.2. This makes it possible for unauthenticated attackers to modify the plugin's site ID settings via the 'cbk_save_v1' AJAX action.	5.3	More Details
CVE-2026-1303	The MailChimp Campaigns plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.2.4. This is due to missing capability checks on the `mailchimp_campaigns_manager_disconnect_app` function that is hooked to the AJAX action of the same name. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect the site from its MailChimp synchronization app, disrupting automated email campaigns and marketing integrations.	5.3	More Details
CVE-2026-26005	ClipBucket v5 is an open source video sharing platform. Prior to 5.5.3 - #45, in Clip Bucket V5, The Remote Play allows creating video entries that reference external video URLs without uploading the video files to the server. However, by specifying an internal network host in the video URL, an SSRF can be triggered, causing GET requests to be sent to internal servers. An attacker can exploit this to scan the internal network. Even a regular (non-privileged) user can carry out the attack.	5.0	More Details
CVE-2026-2555	A weakness has been identified in JeecgBoot 3.9.1. This vulnerability affects the function importDocumentFromZip of the file org/jeecg/modules/airag/llm/controller/AiragKnowledgeController.java of the component Retrieval-Augmented Generation. Executing a manipulation can lead to deserialization. The attack can be launched remotely. Attacks of this nature are highly complex. It is stated that the exploitability is difficult. The project was informed of the problem early through an issue report but has not responded yet.	5.0	More Details
CVE-2026-1249	The MP3 Audio Player – Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to Server-Side Request Forgery in versions 5.3 to 5.10 via the 'load_lyrics_ajax_callback' function. This makes it possible for authenticated attackers, with author 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.	5.0	More Details
CVE-2025-36348	IBM Sterling B2B Integrator versions 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5, and 6.2.1.0 through 6.2.1.1, and IBM Sterling File Gateway versions 6.1.0.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5, and 6.2.1.0 through 6.2.1.1 may expose sensitive information to a remote privileged attacker due to the application returning detailed technical error messages in the browser.	4.9	More Details
CVE-2025-54162	A path traversal vulnerability has been reported to affect File Station 5. If a remote attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5068 and later	4.9	More Details
CVE-2025-13681	The BFG Tools – Extension Zipper plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.0.7. This is due to insufficient input validation on the user-supplied `first_file` parameter in the `zip()` function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files and directories outside the intended `/wp-content/plugins/` directory, which can contain sensitive information such as wp-config.php.	4.9	More Details
CVE-2025-59386	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: QuTS hero h5.3.2.3354 build 20251225 and later	4.9	More Details
CVE-2025-54155	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 5. If a remote attacker gains an administrator account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5018 and later	4.9	More Details
CVE-2025-	An allocation of resources without limits or throttling vulnerability has been reported to affect Qsync Central. If a remote attacker gains an administrator account, they can then exploit the vulnerability to prevent other systems, applications, or	4.9	More

58471	processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: Qsync Central 5.2.0.1 (2025/12/21) and later		Details
CVE-2026-1258	The Mail Mint plugin for WordPress is vulnerable to blind SQL Injection via the 'forms', 'automation', 'email/templates', and 'contacts/import/tutorlms/map' API endpoints in all versions up to, and including, 1.19.2 . This is due to insufficient escaping on the user supplied 'order-by', 'order-type', and 'selectedCourses' parameters and lack of sufficient preparation on the existing SQL queries. This makes it possible for authenticated attackers, with administrator level access and above, to append additional SQL queries into already existing queries.	4.9	More Details
CVE-2025-58472	A NULL pointer dereference vulnerability has been reported to affect Qsync Central. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	4.9	More Details
CVE-2025-54163	A NULL pointer dereference vulnerability has been reported to affect File Station 5. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5166 and later	4.9	More Details
CVE-2026-25964	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.5.1, a Path Traversal vulnerability in the RecipeImport workflow of Tandoor Recipes allows authenticated users with import permissions to read arbitrary files on the server. This vulnerability stems from a lack of input validation in the file_path parameter and insufficient checks in the Local storage backend, enabling an attacker to bypass storage directory restrictions and access sensitive system files (e.g., /etc/passwd) or application configuration files (e.g., settings.py), potentially leading to full system compromise. This vulnerability is fixed in 2.5.1.	4.9	More Details
CVE-2026-57710	An allocation of resources without limits or throttling vulnerability has been reported to affect Qsync Central. If a remote attacker gains an administrator account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	4.9	More Details
CVE-2025-57711	An allocation of resources without limits or throttling vulnerability has been reported to affect Qsync Central. If a remote attacker gains an administrator account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: Qsync Central 5.0.0.4 (2026/01/20) and later	4.9	More Details
CVE-2026-22821	mreporting is the more reporting GLPI plugin. Prior to 1.9.4, there is a possible SQL injection on date change. This vulnerability is fixed in 1.9.4.	4.9	More Details
CVE-2025-58466	A use of uninitialized variable vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to denial of service conditions, or modify control flow in unexpected ways. We have already fixed the vulnerability in the following versions: QTS 5.2.8.3332 build 20251128 and later QuTS hero h5.2.8.3321 build 20251117 and later	4.9	More Details
CVE-2025-66274	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: QuTS hero h5.3.2.3354 build 20251225 and later	4.9	More Details
CVE-2025-54161	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 5. If a remote attacker gains an administrator account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5068 and later	4.9	More Details
CVE-2026-1356	The Converter for Media – Optimize images | Convert WebP & AVIF plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.5.1 via the PassthruLoader::load_image_source function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	4.8	More Details
CVE-2026-2537	A vulnerability was identified in Comfast CF-E4 2.6.0.1. This impacts an unknown function of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone of the component HTTP POST Request Handler. Such manipulation of the argument timestr leads to command injection. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-36597	Dell Avamar, versions prior to 19.12 with patch 338905, contains an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Security. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to information disclosure.	4.7	More Details
CVE-2026-26079	Roundcube Webmail before 1.5.13 and 1.6 before 1.6.13 allows Cascading Style Sheets (CSS) injection, e.g., because comments are mishandled.	4.7	More Details
CVE-2026-20662	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.4, macOS Tahoe 26.3. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2026-20640	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3. An attacker with physical access to iPhone may be able to take and view screenshots of sensitive data from the iPhone during iPhone Mirroring with Mac.	4.6	More Details
CVE-2026-20674	A privacy issue was addressed by removing sensitive data. This issue is fixed in iOS 26.3 and iPadOS 26.3. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details

CVE-2026-1094	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.8 before 18.8.4 that could have allowed an authenticated developer to hide specially crafted file changes from the WebUI.	4.6	More Details
CVE-2026-20605	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, macOS Tahoe 26.3, macOS Sonoma 14.8.4. An app may be able to crash a system process.	4.6	More Details
CVE-2026-20661	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3, iOS 18.7.5 and iPadOS 18.7.5. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2026-20645	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 26.3 and iPadOS 26.3, iOS 18.7.5 and iPadOS 18.7.5. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2025-13333	IBM WebSphere Application Server 9.0, and 8.5 could provide weaker than expected security during system administration of security settings.	4.4	More Details
CVE-2026-2002	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form_name parameter in all versions up to, and including, 1.50.2 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. The plugin allows admins to give form management permissions to lower level users, which could make this exploitable by users such as subscribers.	4.4	More Details
CVE-2025-62855	A path traversal vulnerability has been reported to affect File Station 5. If a local attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5190 and later	4.4	More Details
CVE-2026-20603	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Tahoe 26.3. An app with root privileges may be able to access private information.	4.4	More Details
CVE-2026-0724	The WPlyr Media Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_wplyr_accent_color' parameter in all versions up to, and including, 1.3.0 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-2026-2027	The AMP Enhancer – Compatibility Layer for Official AMP Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the AMP Custom CSS setting in all versions up to, and including, 1.0.49 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-0815	The Category Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag-image' parameter 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 Editor-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-2026-20609	The issue was addressed with improved memory handling. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. Processing a maliciously crafted file may lead to a denial-of-service or potentially disclose memory contents.	4.4	More Details
CVE-2025-15483	The Link Hopper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘hop_name’ parameter in all versions up to, and including, 2.5 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-2026-0693	The Allow HTML in Category Descriptions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via category descriptions in all versions up to, and including, 1.2.4. This is due to the plugin unconditionally removing the `wp_kses_data` output filter for term_description, link_description, link_notes, and user_description fields without checking user capabilities. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in category descriptions that will execute whenever a user accesses a page where the category description is displayed. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-0735	The User Language Switch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tab_color_picker_language_switch' parameter in all versions up to, and including, 1.6.10 due to insufficient input sanitization and output escaping. 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-62856	A path traversal vulnerability has been reported to affect File Station 5. If a local attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5190 and later	4.4	More Details
CVE-2026-1983	The SEATT: Simple Event Attendance plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.0. This is due to missing nonce validation on the event deletion functionality. This makes it possible for unauthenticated attackers to delete arbitrary events 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-	The MDirector Newsletter plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including,		

2025-14852	4.5.8. This is due to missing nonce verification on the mdirectorNewsletterSave function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-14873	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.2.5. This is due to the 'call_by_route_name' function in the routing layer only validating user capabilities without enforcing nonce verification. This makes it possible for unauthenticated attackers to perform multiple administrative actions via forged requests granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-1394	The WP Quick Contact Us plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update 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-2026-1254	The Modula Image Gallery – Photo Grid & Video Gallery plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.13.6. This is due to the plugin not properly verifying that a user is authorized to modify specific posts before updating them via the REST API. This makes it possible for authenticated attackers, with contributor level access and above, to update the title, excerpt, and content of arbitrary posts by passing post IDs in the modulaImages field when editing a gallery.	4.3	More Details
CVE-2023-38005	IBM Cloud Pak System 2.3.3.6, 2.3.3.7, 2.3.4.0, 2.3.4.1, and 2.3.5.0 could allow an authenticated user to perform unauthorized tasks due to improper access controls.	4.3	More Details
CVE-2026-0998	Mattermost versions 11.1.x <= 11.1.2, 10.11.x <= 10.11.9, 11.2.x <= 11.2.1 and Mattermost Plugin Zoom versions <=1.11.0 fail to validate user identity and post ownership in the {{/api/v1/askPMI}} endpoint which allows unauthorized users to start Zoom meetings as any user and overwrite arbitrary posts via direct API calls with manipulated user IDs and post data.. Mattermost Advisory ID: MMSA-2025-00534	4.3	More Details
CVE-2026-1215	The MMA Call Tracking plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3.15. This is due to missing nonce validation when saving plugin configuration on the `mma_call_tracking_menu` admin page. This makes it possible for unauthenticated attackers to modify call tracking configuration 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-2026-0997	Mattermost versions 11.1.x <= 11.1.2, 10.11.x <= 10.11.9, 11.2.x <= 11.2.1 and Mattermost Plugin Zoom versions <=1.11.0 fail to validate the authenticated user when processing {{/plugins/zoom/api/v1/channel-preference}}, which allows any logged-in user to change Zoom meeting restrictions for arbitrary channels via crafted API requests.. Mattermost Advisory ID: MMSA-2025-00558	4.3	More Details
CVE-2025-15524	The Gallery by FooGallery plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ajax_get_gallery_info() function in all versions up to, and including, 3.1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve metadata (name, image count, thumbnail URL) of private, draft, and password-protected galleries by enumerating gallery IDs.	4.3	More Details
CVE-2026-20635	The issue was addressed with improved memory handling. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3, Safari 26.3. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-15520	The RegistrationMagic WordPress plugin before 6.0.7.2 checks nonces but not capabilities, allowing for the disclosure of some sensitive data to subscribers and above.	4.3	More Details
CVE-2026-22892	Mattermost versions 11.1.x <= 11.1.2, 10.11.x <= 10.11.9, 11.2.x <= 11.2.1 fail to validate user permissions when creating Jira issues from Mattermost posts, which allows an authenticated attacker with access to the Jira plugin to read post content and attachments from channels they do not have access to via the /create-issue API endpoint by providing the post ID of an inaccessible post.. Mattermost Advisory ID: MMSA-2025-00550	4.3	More Details
CVE-2026-25531	Kanboard is project management software focused on Kanban methodology. Prior to 1.2.50, The fix for CVE-2023-33968 is incomplete. The TaskCreationController::duplicateProjects() endpoint does not validate user permissions for target projects, allowing authenticated users to duplicate tasks into projects they cannot access. This vulnerability is fixed in 1.2.50.	4.3	More Details
CVE-2026-2323	Inappropriate implementation in Downloads in Google Chrome prior to 145.0.7632.45 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-50618	A Use of Single-factor Authentication vulnerability in the Authentication component of CIPPlanner CIPAce before 9.17 allows attackers to bypass a protection mechanism. When the system is configured to allow login with internal accounts, an attacker can possibly obtain full authentication if the secret in a single-factor authentication scheme gets compromised.	4.3	More Details
CVE-2026-25633	Statamic is a, Laravel + Git powered CMS designed for building websites. Prior to 5.73.6 and 6.2.5, users without permission to view assets are able are able to download them and view their metadata. Logged-out users and users without permission to access the control panel are unable to take advantage of this. This has been fixed in 5.73.6 and 6.2.5.	4.3	More Details
CVE-2026-2032	Malicious scripts that interrupt new tab page loading could cause desynchronization between the address bar and page content, allowing the attacker to spoof arbitrary HTML under a trusted domain. This vulnerability affects Firefox for iOS < 147.2.1.	4.3	More Details
CVE-2026-2608	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on a function in all versions up to, and including, 3.5.32. This makes it possible for authenticated attackers, with Contributor-level access and above, to perform an unauthorized action.	4.3	More Details

CVE-2025-14350	Mattermost versions 11.1.x <= 11.1.2, 10.11.x <= 10.11.9, 11.2.x <= 11.2.1 fail to properly validate team membership when processing channel mentions which allows authenticated users to determine the existence of teams and their URL names via posting channel shortlinks and observing the channel_mentions property in the API response. Mattermost Advisory ID: MMSA-2025-00563	4.3	More Details
CVE-2025-2418	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in TR7 Cyber Defense Inc. Web Application Firewall allows Phishing.This issue affects Web Application Firewall: from 4.30 through 16022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-2022	The Smart Forms plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'rednao_smart_forms_get_campaigns' AJAX action in all versions up to, and including, 2.6.99. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve donation campaign data including campaign IDs and names.	4.3	More Details
CVE-2026-1080	GitLab has remediated an issue in GitLab EE affecting all versions from 16.7 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an authenticated user to access iteration data from private descendant groups by querying the iterations API endpoint.	4.3	More Details
CVE-2026-1748	The Invoct – PDF Invoices & Billing for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on multiple functions in all versions up to, and including, 1.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve invoice clients, invoice items, and list of WordPress users along with their emails.	4.3	More Details
CVE-2026-2003	Improper validation of type "oidvector" in PostgreSQL allows a database user to disclose a few bytes of server memory. We have not ruled out viability of attacks that arrange for presence of confidential information in disclosed bytes, but they seem unlikely. Versions before PostgreSQL 18.2, 17.8, 16.12, 15.16, and 14.21 are affected.	4.3	More Details
CVE-2025-12073	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.0 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions, could have allowed an authenticated user to perform server-side request forgery against internal services by bypassing protections in the Git repository import functionality.	4.3	More Details
CVE-2026-0929	The RegistrationMagic WordPress plugin before 6.0.7.2 does not have proper capability checks, allowing subscribers and above to create forms on the site.	4.3	More Details
CVE-2026-2312	The Media Library Folders plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 8.3.6 via the delete_maxgalleria_media() and maxgalleria_rename_image() functions due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to delete or rename attachments owned by other users (including administrators). The rename flow also deletes all postmeta for the target attachment, causing data loss.	4.3	More Details
CVE-2026-26019	LangChain is a framework for building LLM-powered applications. Prior to 1.1.14, the RecursiveUrlLoader class in @langchain/community is a web crawler that recursively follows links from a starting URL. Its preventOutside option (enabled by default) is intended to restrict crawling to the same site as the base URL. The implementation used String.startsWith() to compare URLs, which does not perform semantic URL validation. An attacker who controls content on a crawled page could include links to domains that share a string prefix with the target, causing the crawler to follow links to attacker-controlled or internal infrastructure. Additionally, the crawler performed no validation against private or reserved IP addresses. A crawled page could include links targeting cloud metadata services, localhost, or RFC 1918 addresses, and the crawler would fetch them without restriction. This vulnerability is fixed in 1.1.14.	4.1	More Details
CVE-2019-25313	FlexNet Publisher 11.12.1 contains a cross-site request forgery vulnerability that allows attackers to create administrative user accounts without authentication. Attackers can craft a malicious HTML form to trick authenticated users into submitting a request that creates a new local admin account with a predefined password.	4.0	More Details
CVE-2025-12755	IBM MQ Operator (SC2 v3.2.0–3.8.1, LTS v2.0.0–2.0.29) and IBM-supplied MQ Advanced container images (across affected SC2, CD, and LTS 9.3.x–9.4.x releases) contain a vulnerability where log messages are not properly neutralized before being written to log files. This flaw could allow an unauthorized user to inject malicious data into MQ log entries, potentially leading to misleading logs, log manipulation, or downstream log-processing issues.	4.0	More Details
CVE-2025-36183	IBM watsonx.data 2.2 through 2.2.1 IBM Lakehouse could allow a privileged user to upload malicious files that could be executed server to modify limited files or data.	3.8	More Details
CVE-2025-14573	Mattermost versions 10.11.x <= 10.11.9 fail to enforce invite permissions when updating team settings, which allows team administrators without proper permissions to bypass restrictions and add users to their team via API requests. Mattermost Advisory ID: MMSA-2025-00561	3.8	More Details
CVE-2026-2618	A vulnerability was determined in Beetel 777VR1 up to 01.00.09. This impacts an unknown function of the component SSH Service. This manipulation causes risky cryptographic algorithm. The attack is possible to be carried out remotely. The attack is considered to have high complexity. The exploitability is said to be difficult. 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.	3.7	More Details
	### Summary The `arrayLimit` option in qs does not enforce limits for comma-separated values when `comma: true` is enabled, allowing attackers to cause denial-of-service via memory exhaustion. This is a bypass of the array limit enforcement, similar to the bracket notation bypass addressed in GHSA-6rw7-vpxm-498p (CVE-2025-15284). ### Details When the `comma` option is set to `true` (not the default, but configurable in applications), qs allows parsing comma-separated strings as arrays (e.g., `?param=a,b,c` becomes `['a', 'b', 'c']`). However, the limit check for `arrayLimit` (default: 20) and the optional throwOnLimitExceeded occur after the comma-handling logic in `parseArrayValue`, enabling a bypass. This permits creation of arbitrarily large arrays from a single parameter, leading to excessive memory allocation. **Vulnerable code** (lib/parse.js: lines ~40-50): ```js if (val && typeof val === 'string' && options.comma && val.indexOf(',') > -1) { return val.split(','); } if (options.throwOnLimitExceeded && currentArrayLength >= options.arrayLimit) { throw new RangeError('Array limit		

CVE-2026-2391	exceeded. Only ' + options.arrayLimit + ' element' + (options.arrayLimit === 1 ? '' : 's') + ' allowed in an array.'); } return val; ``` The `split(',')` returns the array immediately, skipping the subsequent limit check. Downstream merging via `utils.combine` does not prevent allocation, even if it marks overflows for sparse arrays.This discrepancy allows attackers to send a single parameter with millions of commas (e.g., `?param=,,,,,,,...`), allocating massive arrays in memory without triggering limits. It bypasses the intent of `arrayLimit`, which is enforced correctly for indexed (`a[0]=`) and bracket (`a[]=`) notations (the latter fixed in v6.14.1 per GHSA-6rw7-vpxm-498p). ### PoC **Test 1 - Basic bypass:** ``` npm install qs ``` ```js const qs = require('qs'); const payload = 'a=' + ',.repeat(25); // 26 elements after split (bypasses arrayLimit: 5) const options = { comma: true, arrayLimit: 5, throwOnLimitExceeded: true }; try { const result = qs.parse(payload, options); console.log(result.a.length); // Outputs: 26 (bypass successful) } catch (e) { console.log('Limit enforced:', e.message); // Not thrown } ``` **Configuration:** - `comma: true` - `arrayLimit: 5` - `throwOnLimitExceeded: true` Expected: Throws "Array limit exceeded" error. Actual: Parses successfully, creating an array of length 26. ### Impact Denial of Service (DoS) via memory exhaustion.	3.7	More Details
CVE-2025-14592	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.6 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an authenticated user to perform unauthorized operations by submitting GraphQL mutations through the GLQL API endpoint.	3.7	More Details
CVE-2026-2345	Proctorio Chrome Extension is a browser extension used for online proctoring. The extension contains multiple window.addEventListener('message', ...) handlers that do not properly validate the origin of incoming messages. Specifically, an internal messaging bridge processes messages based solely on the presence of a fromWebsite property without verifying the event.origin attribute.	3.6	More Details
CVE-2025-14594	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.11 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that, under certain conditions could have allowed an authenticated user to view certain pipeline values by querying the API.	3.5	More Details
CVE-2026-2547	A vulnerability was detected in LigeroSmart up to 6.1.26. The impacted element is the function AgentDashboard of the file /otrs/index.pl. Performing a manipulation of the argument Subaction results in cross site scripting. Remote exploitation of the attack is possible. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-2545	A weakness has been identified in LigeroSmart up to 6.1.26. Impacted is an unknown function of the file /otrs/index.pl?Action=AgentTicketSearch. This manipulation of the argument Profile causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-2557	A vulnerability was detected in cskefu up to 8.0.1. Impacted is the function Upload of the file com/cskefu/cc/controller/resource/MediaController.java of the component File Upload. The manipulation results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-55271	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in phpgurukul Gym Management System 1.0. This issue is present in the profile update functionality of the User Panel, specifically the /profile.php endpoint.	3.5	More Details
CVE-2026-1282	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.6 before 18.6.6, 18.7 before 18.7.4, and 18.8 before 18.8.4 that could have allowed an authenticated user to inject malicious content into project labels titles.	3.5	More Details
CVE-2026-2622	A vulnerability was detected in Blossom up to 1.17.1. This vulnerability affects the function content of the file blossom-backend/backend/src/main/java/com/blossom/backend/server/article/draft/ArticleController.java of the component Article Title Handler. The manipulation results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-2546	A security vulnerability has been detected in LigeroSmart up to 6.1.26. The affected element is an unknown function of the file /otrs/index.pl. Such manipulation of the argument SortBy leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-20646	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Tahoe 26.3. A malicious app may be able to read sensitive location information.	3.3	More Details
CVE-2026-20656	A logic issue was addressed with improved validation. This issue is fixed in iOS 18.7.5 and iPadOS 18.7.5, Safari 26.3, macOS Tahoe 26.3. An app may be able to access a user's Safari history.	3.3	More Details
CVE-2026-20601	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.3. An app may be able to monitor keystrokes without user permission.	3.3	More Details
CVE-2026-20663	The issue was resolved by sanitizing logging. This issue is fixed in iOS 26.3 and iPadOS 26.3, iOS 18.7.5 and iPadOS 18.7.5. An app may be able to enumerate a user's installed apps.	3.3	More Details
CVE-2026-20681	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Tahoe 26.3. An app may be able to access information about a user's contacts.	3.3	More Details
CVE-2026-20796	Mattermost versions 10.11.x <= 10.11.9 fail to properly validate channel membership at the time of data retrieval which allows a deactivated user to learn team names they should not have access to via a race condition in the /common_teams API endpoint.. Mattermost Advisory ID: MMSA-2025-00549	3.1	More Details

CVE-2026-0102	Under specific conditions, a malicious webpage may trigger autofill population after two consecutive taps, potentially without clear or intentional user consent. This could result in disclosure of stored autofill data such as addresses, email, or phone number metadata.	3.1	More Details
CVE-2026-20671	A logic issue was addressed with improved checks. This issue is fixed in watchOS 26.3, tvOS 26.3, macOS Tahoe 26.3, macOS Sonoma 14.8.4, macOS Sequoia 15.7.4, iOS 18.7.5 and iPadOS 18.7.5, visionOS 26.3, iOS 26.3 and iPadOS 26.3. An attacker in a privileged network position may be able to intercept network traffic.	3.1	More Details
CVE-2026-2543	A vulnerability was identified in vichan-devel vichan up to 5.1.5. This vulnerability affects unknown code of the file inc/mod/pages.php of the component Password Change Handler. The manipulation of the argument Password leads to unverified password change. The attack can be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2026-20642	An input validation issue was addressed. This issue is fixed in iOS 26.3 and iPadOS 26.3. A person with physical access to an iOS device may be able to access photos from the lock screen.	2.4	More Details
CVE-2026-23200	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix ECMP sibling count mismatch when clearing RTF_ADDRCONF syzbot reported a kernel BUG in fib6_add_rt2node() when adding an IPv6 route. [0] Commit f72514b3c569 ("ipv6: clear RA flags when adding a static route") introduced logic to clear RTF_ADDRCONF from existing routes when a static route with the same nexthop is added. However, this causes a problem when the existing route has a gateway. When RTF_ADDRCONF is cleared from a route that has a gateway, that route becomes eligible for ECMP, i.e. rt6_qualify_for_ecmp() returns true. The issue is that this route was never added to the fib6_siblings list. This leads to a mismatch between the following counts: - The sibling count computed by iterating fib6_next chain, which includes the newly ECMP-eligible route - The actual siblings in fib6_siblings list, which does not include that route When a subsequent ECMP route is added, fib6_add_rt2node() hits BUG_ON(sibling->fib6_nsiblings != rt->fib6_nsiblings) because the counts don't match. Fix this by only clearing RTF_ADDRCONF when the existing route does not have a gateway. Routes without a gateway cannot qualify for ECMP anyway (rt6_qualify_for_ecmp() requires fib_nh_gw_family), so clearing RTF_ADDRCONF on them is safe and matches the original intent of the commit. [0]: kernel BUG at net/ipv6/ip6_fib.c:1217! Oops: invalid opcode: 0000 [#1] SMP KASAN PTI CPU: 0 UID: 0 PID: 6010 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025 RIP: 0010:fib6_add_rt2node+0x3433/0x3470 net/ipv6/ip6_fib.c:1217 [...] Call Trace: <TASK> fib6_add+0x8da/0x18a0 net/ipv6/ip6_fib.c:1532 __ip6_ins_rt net/ipv6/route.c:1351 [inline] ip6_route_add+0xde/0x1b0 net/ipv6/route.c:3946 ipv6_route_ioctl+0x35c/0x480 net/ipv6/route.c:4571 inet6_ioctl+0x219/0x280 net/ipv6/af_inet6.c:577 sock_do_ioctl+0xdc/0x300 net/socket.c:1245 sock_ioctl+0x576/0x790 net/socket.c:1366 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xfa/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f	N/A	More Details
CVE-2026-23199	In the Linux kernel, the following vulnerability has been resolved: procfs: avoid fetching build ID while holding VMA lock Fix PROCMAP_QUERY to fetch optional build ID only after dropping mmap_lock or per-VMA lock, whichever was used to lock VMA under question, to avoid deadlock reported by syzbot: -> #1 (&mm->mmap_lock){++++}-{4:4}: __might_fault+0xed/0x170 _copy_to_iter+0x118/0x1720 copy_page_to_iter+0x12d/0x1e0 filemap_read+0x720/0x10a0 blkdev_read_iter+0x2b5/0x4e0 vfs_read+0x7f4/0xae0 ksys_read+0x12a/0x250 do_syscall_64+0xcb/0xf80 entry_SYSCALL_64_after_hwframe+0x77/0x7f -> #0 (&sb->s_type->i_mutex_key#8){++++}-{4:4}: __lock_acquire+0x1509/0x26d0 lock_acquire+0x185/0x340 down_read+0x98/0x490 blkdev_read_iter+0x2a7/0x4e0 __kernel_read+0x39a/0xa90 freader_fetch+0x1d5/0xa80 __build_id_parse.isra.0+0xea/0x6a0 do_procmap_query+0xd75/0x1050 procfs_procmap_ioctl+0x7a/0xb0 __x64_sys_ioctl+0x18e/0x210 do_syscall_64+0xcb/0xf80 entry_SYSCALL_64_after_hwframe+0x77/0x7f other info that might help us debug this: Possible unsafe locking scenario: CPU0 CPU1 ---- ---- rlock(&mm->mmap_lock); lock(&sb->s_type->i_mutex_key#8); lock(&mm->mmap_lock); rlock(&sb->s_type->i_mutex_key#8); *** DEADLOCK *** This seems to be exacerbated (as we haven't seen these syzbot reports before that) by the recent: 777a8560fd29 ("lib/buildid: use __kernel_read() for sleepable context") To make this safe, we need to grab file refcount while VMA is still locked, but other than that everything is pretty straightforward. Internal build_id_parse() API assumes VMA is passed, but it only needs the underlying file reference, so just add another variant build_id_parse_file() that expects file passed directly. [akpm@linux-foundation.org: fix up kerneldoc]	N/A	More Details
CVE-2026-23198	In the Linux kernel, the following vulnerability has been resolved: KVM: Don't clobber irqfd routing type when deassigning irqfd When deassigning a KVM_IRQFD, don't clobber the irqfd's copy of the IRQ's routing entry as doing so breaks kvm_arch_irq_bypass_del_producer() on x86 and arm64, which explicitly look for KVM_IRQ_ROUTING_MSI. Instead, to handle a concurrent routing update, verify that the irqfd is still active before consuming the routing information. As evidenced by the x86 and arm64 bugs, and another bug in kvm_arch_update_irqfd_routing() (see below), clobbering the entry type without notifying arch code is surprising and error prone. As a bonus, checking that the irqfd is active provides a convenient location for documenting _why_ KVM must not consume the routing entry for an irqfd that is in the process of being deassigned: once the irqfd is deleted from the list (which happens *before* the eventfd is detached), it will no longer receive updates via kvm_irq_routing_update(), and so KVM could deliver an event using stale routing information (relative to KVM_SET_GSI_ROUTING returning to userspace). As an even better bonus, explicitly checking for the irqfd being active fixes a similar bug to the one the clobbering is trying to prevent: if an irqfd is deactivated, and then its routing is changed, kvm_irq_routing_update() won't invoke kvm_arch_update_irqfd_routing() (because the irqfd isn't in the list). And so if the irqfd is in bypass mode, IRQs will continue to be posted using the old routing information. As for kvm_arch_irq_bypass_del_producer(), clobbering the routing type results in KVM incorrectly keeping the IRQ in bypass mode, which is especially problematic on AMD as KVM tracks IRQs that are being posted to a vCPU in a list whose lifetime is tied to the irqfd. Without the help of KASAN to detect use-after-free, the most common sympton on AMD is a NULL pointer deref in amd_iommu_update_ga() due to the memory for irqfd structure being re-allocated and zeroed, resulting in irqfd->irq_bypass_data being NULL when read by avic_update_iommu_vcpu_affinity(): BUG: kernel NULL pointer dereference, address: 0000000000000018 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 40cf2b9067 P4D 40cf2b9067 PUD 408362a067 PMD 0 Oops: Oops: 0000 [#1] SMP CPU: 6 UID: 0 PID: 40383 Comm: vfio_irq_test Tainted: G U W O 6.19.0-smp--5dddc257e6b2-irqfd #31 NONE Tainted: [U]=USER, [W]=WARN, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 34.78.2-0 09/05/2025 RIP: 0010:amd_iommu_update_ga+0x19/0xe0 Call Trace: <TASK> avic_update_iommu_vcpu_affinity+0x3d/0x90 [kvm_amd] __avic_vcpu_load+0xf4/0x130 [kvm_amd] kvm_arch_vcpu_load+0x89/0x210 [kvm] vcpu_load+0x30/0x40 [kvm] kvm_arch_vcpu_ioctl_run+0x45/0x620 [kvm]	N/A	More Details

	kvm_vcpu_ioctl+0x571/0x6a0 [kvm] __se_sys_ioctl+0x6d/0xb0 do_syscall_64+0x6f/0x9d0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x46893b </TASK> ---[end trace 0000000000000000]--- If AVIC is inhibited when the irfd is deassigned, the bug will manifest as list corruption, e.g. on the next irqfd assignment. list_add corruption. next->prev should be prev (ffff8d474d5cd588), but was 0000000000000000. (next=ffff8d8658f86530). ----------[cut here]---------- kernel BUG at lib/list_debug.c:31! Oops: invalid opcode: 0000 [#1] SMP CPU: 128 UID: 0 PID: 80818 Comm: vfio_irq_test Tainted: G U W O 6.19.0-smp--f19dc4d680ba-irqfd #28 NONE Tainted: [U]=USER, [W]=WARN, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 34.78.2-0 09/05/2025 RIP: 0010:__list_add_valid_or_report+0x97/0xc0 Call Trace: <TASK> avic_pi_update_irte+0x28e/0x2b0 [kvm_amd] kvm_pi_update_irte+0xbf/0x190 [kvm] kvm_arch_irq_bypass_add_producer+0x72/0x90 [kvm] irq_bypass_register_consumer+0xcd/0x170 [irqbypa ---truncated---		
CVE-2026-23189	In the Linux kernel, the following vulnerability has been resolved: ceph: fix NULL pointer dereference in ceph_mds_auth_match() The CephFS kernel client has regression starting from 6.18-rc1. We have issue in ceph_mds_auth_match() if fs_name == NULL: const char fs_name = mdsc->fsc->mount_options->mds_namespace; ... if (auth->match.fs_name && strcmp(auth->match.fs_name, fs_name)) { / fsname mismatch, try next one */ return 0; } Patrick Donnelly suggested that: In summary, we should definitely start decoding `fs_name` from the MDSMap and do strict authorizations checks against it. Note that the `-o mds_namespace=foo` should only be used for selecting the file system to mount and nothing else. It's possible no mds_namespace is specified but the kernel will mount the only file system that exists which may have name "foo". This patch reworks ceph_mdsmap_decode() and namespace_equals() with the goal of supporting the suggested concept. Now struct ceph_mdsmap contains m_fs_name field that receives copy of extracted FS name by ceph_extract_encoded_string(). For the case of "old" CephFS file systems, it is used "cephfs" name. [idryomov: replace redundant %*pE with %s in ceph_mdsmap_decode(), get rid of a series of strlen() calls in ceph_namespace_match(), drop changes to namespace_equals() body to avoid treating empty mds_namespace as equal, drop changes to ceph_mdsc_handle_fsmap() as namespace_equals() isn't an equivalent substitution there]	N/A	More Details
CVE-2026-23197	In the Linux kernel, the following vulnerability has been resolved: i2c: imx: preserve error state in block data length handler When a block read returns an invalid length, zero or >I2C_SMBUS_BLOCK_MAX, the length handler sets the state to IMX_I2C_STATE_FAILED. However, i2c_imx_master_isr() unconditionally overwrites this with IMX_I2C_STATE_READ_CONTINUE, causing an endless read loop that overruns buffers and crashes the system. Guard the state transition to preserve error states set by the length handler.	N/A	More Details
CVE-2026-23196	In the Linux kernel, the following vulnerability has been resolved: HID: Intel-thc-hid: Intel-thc: Add safety check for reading DMA buffer Add DMA buffer readiness check before reading DMA buffer to avoid unexpected NULL pointer accessing.	N/A	More Details
CVE-2026-23195	In the Linux kernel, the following vulnerability has been resolved: cgroup/dmem: avoid pool UAF An UAF issue was observed: BUG: KASAN: slab-use-after-free in page_counter_uncharge+0x65/0x150 Write of size 8 at addr ffff888106715440 by task insmod/527 CPU: 4 UID: 0 PID: 527 Comm: insmod 6.19.0-rc7-next-20260129+ #11 Tainted: [O]=OOT_MODULE Call Trace: <TASK> dump_stack_lvl+0x82/0xd0 kasan_report+0xca/0x100 kasan_check_range+0x39/0x1c0 page_counter_uncharge+0x65/0x150 dmem_cgroup_uncharge+0x1f/0x260 Allocated by task 527: Freed by task 0: The buggy address belongs to the object at ffff888106715400 which belongs to the cache kmalloc-512 of size 512 The buggy address is located 64 bytes inside of freed 512-byte region [ffff888106715400, ffff888106715600) The buggy address belongs to the physical page: Memory state around the buggy address: ffff888106715300: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffff888106715380: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc >ffff888106715400: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff888106715480: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff888106715500: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb The issue occurs because a pool can still be held by a caller after its associated memory region is unregistered. The current implementation frees the pool even if users still hold references to it (e.g., before uncharge operations complete). This patch adds a reference counter to each pool, ensuring that a pool is only freed when its reference count drops to zero.	N/A	More Details
CVE-2026-23201	In the Linux kernel, the following vulnerability has been resolved: ceph: fix oops due to invalid pointer for kfree() in parse_longname() This fixes a kernel oops when reading ceph snapshot directories (.snap), for example by simply running `ls /mnt/my_ceph/.snap`. The variable str is guarded by __free(kfree), but advanced by one for skipping the initial '_' in snapshot names. Thus, kfree() is called with an invalid pointer. This patch removes the need for advancing the pointer so kfree() is called with correct memory pointer. Steps to reproduce: 1. Create snapshots on a cephfs volume (I've 63 snaps in my testcase) 2. Add cephfs mount to fstab $ echo "samba-fileserver@.files=/volumes/datapool/stuff/3461082b-ecc9-4e82-8549-3fd2590d3fb6 /mnt/test/stuff ceph acl,noatime,_netdev 0 0" >> /etc/fstab 3. Reboot the system $ systemctl reboot 4. Check if it's really mounted $ mount | grep stuff 5. List snapshots (expected 63 snapshots on my system) $ ls /mnt/test/stuff/.snap Now ls hangs forever and the kernel log shows the oops.	N/A	More Details
CVE-2026-23202	In the Linux kernel, the following vulnerability has been resolved: spi: tegra210-quad: Protect curr_xfer in tegra_qspi_combined_seq_xfer The curr_xfer field is read by the IRQ handler without holding the lock to check if a transfer is in progress. When clearing curr_xfer in the combined sequence transfer loop, protect it with the spinlock to prevent a race with the interrupt handler. Protect the curr_xfer clearing at the exit path of tegra_qspi_combined_seq_xfer() with the spinlock to prevent a race with the interrupt handler that reads this field. Without this protection, the IRQ handler could read a partially updated curr_xfer value, leading to NULL pointer dereference or use-after-free.	N/A	More Details
CVE-2026-23194	In the Linux kernel, the following vulnerability has been resolved: rust_binder: correctly handle FDA objects of length zero Fix a bug where an empty FDA (fd array) object with 0 fds would cause an out-of-bounds error. The previous implementation used `skip == 0` to mean "this is a pointer fixup", but 0 is also the correct skip length for an empty FDA. If the FDA is at the end of the buffer, then this results in an attempt to write 8-bytes out of bounds. This is caught and results in an EINVAL error being returned to userspace. The pattern of using `skip == 0` as a special value originates from the C-implementation of Binder. As part of fixing this bug, this pattern is replaced with a Rust enum. I considered the alternate option of not pushing a fixup when the length is zero, but I think it's cleaner to just get rid of the zero-is-special stuff. The root cause of this bug was diagnosed by Gemini CLI on first try. I used the following prompt: > There appears to be a bug in @drivers/android/binder/thread.rs where > the Fixups oob bug is triggered with 316 304 316 324. This implies > that we somehow ended up with a fixup where buffer A has a pointer to > buffer B, but the pointer is located at an index in buffer A that is > out of bounds. Please investigate the code to find the bug. You may > compare with @drivers/android/binder.c that implements this correctly.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Fix use-after-free in iscsit_dec_session_usage_count() In iscsit_dec_session_usage_count(), the function calls complete() while holding the sess-		

CVE-2026-23193	>session_usage_lock. Similar to the connection usage count logic, the waiter signaled by complete() (e.g., in the session release path) may wake up and free the iscsit_session structure immediately. This creates a race condition where the current thread may attempt to execute spin_unlock_bh() on a session structure that has already been deallocated, resulting in a KASAN slab-use-after-free. To resolve this, release the session_usage_lock before calling complete() to ensure all dereferences of the sess pointer are finished before the waiter is allowed to proceed with deallocation.	N/A	More Details
CVE-2026-23192	In the Linux kernel, the following vulnerability has been resolved: linkwatch: use __dev_put() in callers to prevent UAF After linkwatch_do_dev() calls __dev_put() to release the linkwatch reference, the device refcount may drop to 1. At this point, netdev_run_todo() can proceed (since linkwatch_sync_dev() sees an empty list and returns without blocking), wait for the refcount to become 1 via netdev_wait_allrefs_any(), and then free the device via kobject_put(). This creates a use-after-free when __linkwatch_run_queue() tries to call netdev_unlock_ops() on the already-freed device. Note that adding netdev_lock_ops()/netdev_unlock_ops() pair in netdev_run_todo() before kobject_put() would not work, because netdev_lock_ops() is conditional - it only locks when netdev_need_ops_lock() returns true. If the device doesn't require ops_lock, linkwatch won't hold any lock, and netdev_run_todo() acquiring the lock won't provide synchronization. Fix this by moving __dev_put() from linkwatch_do_dev() to its callers. The device reference logically pairs with de-listing the device, so it's reasonable for the caller that did the de-listing to release it. This allows placing __dev_put() after all device accesses are complete, preventing UAF. The bug can be reproduced by adding mdelay(2000) after linkwatch_do_dev() in __linkwatch_run_queue(), then running: ip tuntap add mode tun name tun_test ip link set tun_test up ip link set tun_test carrier off ip link set tun_test carrier on sleep 0.5 ip tuntap del mode tun name tun_test KASAN report: == BUG: KASAN: use-after-free in netdev_need_ops_lock include/net/netdev_lock.h:33 [inline] BUG: KASAN: use-after-free in netdev_unlock_ops include/net/netdev_lock.h:47 [inline] BUG: KASAN: use-after-free in __linkwatch_run_queue+0x865/0x8a0 net/core/link_watch.c:245 Read of size 8 at addr ffff88804de5c008 by task kworker/u32:10/8123 CPU: 0 UID: 0 PID: 8123 Comm: kworker/u32:10 Not tainted syzkaller #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Workqueue: events_unbound linkwatch_event Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x100/0x190 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x156/0x4c9 mm/kasan/report.c:482 kasan_report+0xdf/0x1a0 mm/kasan/report.c:595 netdev_need_ops_lock include/net/netdev_lock.h:33 [inline] netdev_unlock_ops include/net/netdev_lock.h:47 [inline] __linkwatch_run_queue+0x865/0x8a0 net/core/link_watch.c:245 linkwatch_event+0x8f/0xc0 net/core/link_watch.c:304 process_one_work+0x9c2/0x1840 kernel/workqueue.c:3257 process_scheduled_works kernel/workqueue.c:3340 [inline] worker_thread+0x5da/0xe40 kernel/workqueue.c:3421 kthread+0x3b3/0x730 kernel/kthread.c:463 ret_from_fork+0x754/0xaf0 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:246 </TASK> ==	N/A	More Details
CVE-2026-23191	In the Linux kernel, the following vulnerability has been resolved: ALSA: aloop: Fix racy access at PCM trigger The PCM trigger callback of aloop driver tries to check the PCM state and stop the stream of the tied substream in the corresponding cable. Since both check and stop operations are performed outside the cable lock, this may result in UAF when a program attempts to trigger frequently while opening/closing the tied stream, as spotted by fuzzers. For addressing the UAF, this patch changes two things: - It covers the most of code in loopback_check_format() with cable->lock spinlock, and add the proper NULL checks. This avoids already some racy accesses. - In addition, now we try to check the state of the capture PCM stream that may be stopped in this function, which was the major pain point leading to UAF.	N/A	More Details
CVE-2026-23190	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: fix memory leak in acp3x pdm dma ops	N/A	More Details
CVE-2026-23188	In the Linux kernel, the following vulnerability has been resolved: net: usb: r8152: fix resume reset deadlock rtl8152 can trigger device reset during reset which potentially can result in a deadlock: **** DPM device timeout after 10 seconds; 15 seconds until panic **** Call Trace: <TASK> schedule+0x483/0x1370 schedule_preempt_disabled+0x15/0x30 __mutex_lock_common+0x1fd/0x470 __rtl8152_set_mac_address+0x80/0x1f0 dev_set_mac_address+0x7f/0x150 rtl8152_post_reset+0x72/0x150 usb_reset_device+0x1d0/0x220 rtl8152_resume+0x99/0xc0 usb_resume_interface+0x3e/0xc0 usb_resume_both+0x104/0x150 usb_resume+0x22/0x110 The problem is that rtl8152 resume calls reset under tp->control mutex while reset basically re-enters rtl8152 and attempts to acquire the same tp->control lock once again. Reset INACCESSIBLE device outside of tp->control mutex scope to avoid recursive mutex_lock() deadlock.	N/A	More Details
CVE-2026-23204	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_u32: use skb_header_pointer_careful() skb_header_pointer() does not fully validate negative @offset values. Use skb_header_pointer_careful() instead. GangMin Kim provided a report and a repro fooling u32_classify(): BUG: KASAN: slab-out-of-bounds in u32_classify+0x1180/0x11b0 net/sched/cls_u32.c:221	N/A	More Details
CVE-2026-23187	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx8m-blk-ctrl: fix out-of-range access of bc->domains Fix out-of-range access of bc->domains in imx8m_blk_ctrl_remove().	N/A	More Details
CVE-2025-71223	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix refcount leak in smb2_open() When ksmbd_vfs_getattr() fails, the reference count of ksmbd_file must be released.	N/A	More Details
CVE-2025-71224	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: ocb: skip rx_no_sta when interface is not joined ieee80211_ocb_rx_no_sta() assumes a valid channel context, which is only present after JOIN_OCB. RX may run before JOIN_OCB is executed, in which case the OCB interface is not operational. Skip RX peer handling when the interface is not joined to avoid warnings in the RX path.	N/A	More Details
CVE-2026-23174	In the Linux kernel, the following vulnerability has been resolved: nvme-pci: handle changing device dma map requirements The initial state of dma_needs_unmap may be false, but change to true while mapping the data iterator. Enabling swiotlb is one such case that can change the result. The nvme driver needs to save the mapped dma vectors to be unmapped later, so allocate as needed during iteration rather than assume it was always allocated at the beginning. This fixes a NULL dereference from accessing an uninitialized dma_vecs when the device dma unmapping requirements change mid-iteration.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: cpsw: Execute ndo_set_rx_mode callback in a work queue		

CVE-2026-23175	Commit 1767bb2d47b7 ("ipv6: mcast: Don't hold RTNL for IPV6_ADD_MEMBERSHIP and MCAST_JOIN_GROUP.") removed the RTNL lock for IPV6_ADD_MEMBERSHIP and MCAST_JOIN_GROUP operations. However, this change triggered the following call trace on my BeagleBone Black board: WARNING: net/8021q/vlan_core.c:236 at vlan_for_each+0x120/0x124, CPU#0: rpcbind/481 RTNL: assertion failed at net/8021q/vlan_core.c (236) Modules linked in: CPU: 0 UID: 997 PID: 481 Comm: rpcbind Not tainted 6.19.0-rc7-next-20260130-yocto-standard+ #35 PREEMPT Hardware name: Generic AM33XX (Flattened Device Tree) Call trace: unwind_backtrace from show_stack+0x28/0x2c show_stack from dump_stack_lvl+0x30/0x38 dump_stack_lvl from __warn+0xb8/0x11c __warn from warn_slowpath_fmt+0x130/0x194 warn_slowpath_fmt from vlan_for_each+0x120/0x124 vlan_for_each from cpsw_add_mc_addr+0x54/0x98 cpsw_add_mc_addr from __hw_addr_ref_sync_dev+0xc4/0xec __hw_addr_ref_sync_dev from __dev_mc_add+0x78/0x88 __dev_mc_add from igmp6_group_added+0x84/0xec igmp6_group_added from __ipv6_dev_mc_inc+0x1fc/0x2f0 __ipv6_dev_mc_inc from __ipv6_sock_mc_join+0x124/0x1b4 __ipv6_sock_mc_join from do_ipv6_setsockopt+0x84c/0x1168 do_ipv6_setsockopt from ipv6_setsockopt+0x88/0xc8 ipv6_setsockopt from do_sock_setsockopt+0xe8/0x19c do_sock_setsockopt from __sys_setsockopt+0x84/0xac __sys_setsockopt from ret_fast_syscall+0x0/0x54 This trace occurs because vlan_for_each() is called within cpsw_ndo_set_rx_mode(), which expects the RTNL lock to be held. Since modifying vlan_for_each() to operate without the RTNL lock is not straightforward, and because ndo_set_rx_mode() is invoked both with and without the RTNL lock across different code paths, simply adding rtnl_lock() in cpsw_ndo_set_rx_mode() is not a viable solution. To resolve this issue, we opt to execute the actual processing within a work queue, following the approach used by the icssg-prueth driver. Please note: To reproduce this issue, I manually reverted the changes to am335x-bone-common.dtsi from commit c477358e66a3 ("ARM: dts: am335x-bone: switch to new cpsw switch drv") in order to revert to the legacy cpsw driver.	N/A	More Details
CVE-2026-23176	In the Linux kernel, the following vulnerability has been resolved: platform/x86: toshiba_haps: Fix memory leaks in add/remove routines toshiba_haps_add() leaks the haps object allocated by it if it returns an error after allocating that object successfully. toshiba_haps_remove() does not free the object pointed to by toshiba_haps before clearing that pointer, so it becomes unreachable allocated memory. Address these memory leaks by using devm_kzalloc() for allocating the memory in question.	N/A	More Details
CVE-2026-23177	In the Linux kernel, the following vulnerability has been resolved: mm, shmem: prevent infinite loop on truncate race When truncating a large swap entry, shmem_free_swap() returns 0 when the entry's index doesn't match the given index due to lookup alignment. The failure fallback path checks if the entry crosses the end border and aborts when it happens, so truncate won't erase an unexpected entry or range. But one scenario was ignored. When `index` points to the middle of a large swap entry, and the large swap entry doesn't go across the end border, find_get_entries() will return that large swap entry as the first item in the batch with `indices[0]` equal to `index`. The entry's base index will be smaller than `indices[0]`, so shmem_free_swap() will fail and return 0 due to the "base < index" check. The code will then call shmem_confirm_swap(), get the order, check if it crosses the END boundary (which it doesn't), and retry with the same index. The next iteration will find the same entry again at the same index with same indices, leading to an infinite loop. Fix this by retrying with a round-down index, and abort if the index is smaller than the truncate range.	N/A	More Details
CVE-2026-23178	In the Linux kernel, the following vulnerability has been resolved: HID: i2c-hid: fix potential buffer overflow in i2c_hid_get_report() `i2c_hid_xfer` is used to read `recv_len + sizeof(__le16)` bytes of data into `ihid->rawbuf`. The former can come from the userspace in the hidraw driver and is only bounded by HID_MAX_BUFFER_SIZE(16384) by default (unless we also set `max_buffer_size` field of `struct hid_ll_driver` which we do not). The latter has size determined at runtime by the maximum size of different report types you could receive on any particular device and can be a much smaller value. Fix this by truncating `recv_len` to `ihid->bufsize - sizeof(__le16)`. The impact is low since access to hidraw devices requires root.	N/A	More Details
CVE-2026-23179	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: fixup hang in nvmet_tcp_listen_data_ready() When the socket is closed while in TCP_LISTEN a callback is run to flush all outstanding packets, which in turns calls nvmet_tcp_listen_data_ready() with the sk_callback_lock held. So we need to check if we are in TCP_LISTEN before attempting to get the sk_callback_lock() to avoid a deadlock.	N/A	More Details
CVE-2026-23180	In the Linux kernel, the following vulnerability has been resolved: dpaa2-switch: add bounds check for if_id in IRQ handler The IRQ handler extracts if_id from the upper 16 bits of the hardware status register and uses it to index into ethsw->ports[] without validation. Since if_id can be any 16-bit value (0-65535) but the ports array is only allocated with sw_attr.num_ifs elements, this can lead to an out-of-bounds read potentially. Add a bounds check before accessing the array, consistent with the existing validation in dpaa2_switch_rx().	N/A	More Details
CVE-2026-23181	In the Linux kernel, the following vulnerability has been resolved: btrfs: sync read disk super and set block size When the user performs a btrfs mount, the block device is not set correctly. The user sets the block size of the block device to 0x4000 by executing the BLKBSZSET command. Since the block size change also changes the mapping->flags value, this further affects the result of the mapping_min_folio_order() calculation. Let's analyze the following two scenarios: Scenario 1: Without executing the BLKBSZSET command, the block size is 0x1000, and mapping_min_folio_order() returns 0; Scenario 2: After executing the BLKBSZSET command, the block size is 0x4000, and mapping_min_folio_order() returns 2. do_read_cache_folio() allocates a folio before the BLKBSZSET command is executed. This results in the allocated folio having an order value of 0. Later, after BLKBSZSET is executed, the block size increases to 0x4000, and the mapping_min_folio_order() calculation result becomes 2. This leads to two undesirable consequences: 1. filemap_add_folio() triggers a VM_BUG_ON_FOLIO(folio_order(folio) < mapping_min_folio_order(mapping)) assertion. 2. The syzbot report [1] shows a null pointer dereference in create_empty_buffers() due to a buffer head allocation failure. Synchronization should be established based on the inode between the BLKBSZSET command and read cache page to prevent inconsistencies in block size or mapping flags before and after folio allocation. [1] KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:create_empty_buffers+0x4d/0x480 fs/buffer.c:1694 Call Trace: folio_create_buffers+0x109/0x150 fs/buffer.c:1802 block_read_full_folio+0x14c/0x850 fs/buffer.c:2403 filemap_read_folio+0xc8/0x2a0 mm/filemap.c:2496 do_read_cache_folio+0x266/0x5c0 mm/filemap.c:4096 do_read_cache_page mm/filemap.c:4162 [inline] read_cache_page_gfp+0x29/0x120 mm/filemap.c:4195 btrfs_read_disk_super+0x192/0x500 fs/btrfs/volumes.c:1367	N/A	More Details
CVE-2026-23182	In the Linux kernel, the following vulnerability has been resolved: spi: tegra: Fix a memory leak in tegra_slink_probe() In tegra_slink_probe(), when platform_get_irq() fails, it directly returns from the function with an error code, which causes a memory leak. Replace it with a goto label to ensure proper cleanup.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: cgroup/dmem: fix NULL pointer dereference when setting max An issue was triggered: BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 15 UID: 0 PID: 658 Comm: bash Tainted: 6.19.0-rc6-next-2026012 Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (i440FX +		

CVE-2026-23183	PIIX, 1996), RIP: 0010:strcmp+0x10/0x30 RSP: 0018:ffffc900017f7dc0 EFLAGS: 00000246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff888107cd4358 RDX: 0000000019f73907 RSI: ffffffff82cc381a RDI: 0000000000000000 RBP: ffff8881016bef0d R08: 000000006c0e7145 R09: 0000000056c0e714 R10: 0000000000000001 R11: ffff888107cd4358 R12: 0007ffffffffffff R13: ffff888101399200 R14: ffff888100fcb360 R15: 0007ffffffffffff CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 0000000105c79000 CR4: 00000000000006f0 Call Trace: <TASK> dmemcg_limit_write.constprop.0+0x16d/0x390 ? __pfx_set_resource_max+0x10/0x10 kernfs_fop_write_iter+0x14e/0x200 vfs_write+0x367/0x510 ksys_write+0x66/0xe0 do_syscall_64+0x6b/0x390 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f42697e1887 It was trriggered setting max without limitation, the command is like: "echo test/region0 > dmem.max". To fix this issue, add check whether options is valid after parsing the region_name.	N/A	More Details
CVE-2026-23184	In the Linux kernel, the following vulnerability has been resolved: binder: fix UAF in binder_netlink_report() Oneway transactions sent to frozen targets via binder_proc_transaction() return a BR_TRANSACTION_PENDING_FROZEN error but they are still treated as successful since the target is expected to thaw at some point. It is then not safe to access 't' after BR_TRANSACTION_PENDING_FROZEN errors as the transaction could have been consumed by the now thawed target. This is the case for binder_netlink_report() which derreferences 't' after a pending frozen error, as pointed out by the following KASAN report: == BUG: KASAN: slab-use-after-free in binder_netlink_report.isra.0+0x694/0x6c8 Read of size 8 at addr ffff00000f98ba38 by task binder-util/522 CPU: 4 UID: 0 PID: 522 Comm: binder-util Not tainted 6.19.0-rc6-00015-gc03e9c42ae8f #1 PREEMPT Hardware name: linux,dummy-virt (DT) Call trace: binder_netlink_report.isra.0+0x694/0x6c8 binder_transaction+0x66e4/0x79b8 binder_thread_write+0xab4/0x4440 binder_ioctl+0x1fd4/0x2940 [...] Allocated by task 522: __kmalloc_cache_noprof+0x17c/0x50c binder_transaction+0x584/0x79b8 binder_thread_write+0xab4/0x4440 binder_ioctl+0x1fd4/0x2940 [...] Freed by task 488: kfree+0x1d0/0x420 binder_free_transaction+0x150/0x234 binder_thread_read+0x2d08/0x3ce4 binder_ioctl+0x488/0x2940 [...] == Instead, make a transaction copy so the data can be safely accessed by binder_netlink_report() after a pending frozen error. While here, add a comment about not using t->buffer in binder_netlink_report().	N/A	More Details
CVE-2026-23185	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mld: cancel mlo_scan_start_wk mlo_scan_start_wk is not canceled on disconnection. In fact, it is not canceled anywhere except in the restart cleanup, where we don't really have to. This can cause an init-after-queue issue: if, for example, the work was queued and then drv_change_interface got executed. This can also cause use-after-free: if the work is executed after the vif is freed.	N/A	More Details
CVE-2026-23186	In the Linux kernel, the following vulnerability has been resolved: hwmon: (acpi_power_meter) Fix deadlocks related to acpi_power_meter_notify() The acpi_power_meter driver's .notify() callback function, acpi_power_meter_notify(), calls hwmon_device_unregister() under a lock that is also acquired by callbacks in sysfs attributes of the device being unregistered which is prone to deadlocks between sysfs access and device removal. Address this by moving the hwmon device removal in acpi_power_meter_notify() outside the lock in question, but notice that doing it alone is not sufficient because two concurrent METER_NOTIFY_CONFIG notifications may be attempting to remove the same device at the same time. To prevent that from happening, add a new lock serializing the execution of the switch () statement in acpi_power_meter_notify(). For simplicity, it is a static mutex which should not be a problem from the performance perspective. The new lock also allows the hwmon_device_register_with_info() in acpi_power_meter_notify() to be called outside the inner lock because it prevents the other notifications handled by that function from manipulating the "resource" object while the hwmon device based on it is being registered. The sending of ACPI netlink messages from acpi_power_meter_notify() is serialized by the new lock too which generally helps to ensure that the order of handling firmware notifications is the same as the order of sending netlink messages related to them. In addition, notice that hwmon_device_register_with_info() may fail in which case resource->hwmon_dev will become an error pointer, so add checks to avoid attempting to unregister the hwmon device pointer to by it in that case to acpi_power_meter_notify() and acpi_power_meter_remove().	N/A	More Details
CVE-2026-23203	In the Linux kernel, the following vulnerability has been resolved: net: cpsw_new: Execute ndo_set_rx_mode callback in a work queue Commit 1767bb2d47b7 ("ipv6: mcast: Don't hold RTNL for IPV6_ADD_MEMBERSHIP and MCAST_JOIN_GROUP.") removed the RTNL lock for IPV6_ADD_MEMBERSHIP and MCAST_JOIN_GROUP operations. However, this change triggered the following call trace on my BeagleBone Black board: WARNING: net/8021q/vlan_core.c:236 at vlan_for_each+0x120/0x124, CPU#0: rpcbind/496 RTNL: assertion failed at net/8021q/vlan_core.c (236) Modules linked in: CPU: 0 UID: 997 PID: 496 Comm: rpcbind Not tainted 6.19.0-rc6-next-20260122-yocto-standard+ #8 PREEMPT Hardware name: Generic AM33XX (Flattened Device Tree) Call trace: unwind_backtrace from show_stack+0x28/0x2c show_stack from dump_stack_lvl+0x30/0x38 dump_stack_lvl from __warn+0xb8/0x11c __warn from warn_slowpath_fmt+0x130/0x194 warn_slowpath_fmt from vlan_for_each+0x120/0x124 vlan_for_each from cpsw_add_mc_addr+0x54/0xd8 cpsw_add_mc_addr from __hw_addr_ref_sync_dev+0xc4/0xec __hw_addr_ref_sync_dev from __dev_mc_add+0x78/0x88 __dev_mc_add from igmp6_group_added+0x84/0xec igmp6_group_added from __ipv6_dev_mc_inc+0x1fc/0x2f0 __ipv6_dev_mc_inc from __ipv6_sock_mc_join+0x124/0x1b4 __ipv6_sock_mc_join from do_ipv6_setsockopt+0x84c/0x1168 do_ipv6_setsockopt from ipv6_setsockopt+0x88/0xc8 ipv6_setsockopt from do_sock_setsockopt+0xe8/0x19c do_sock_setsockopt from __sys_setsockopt+0x84/0xac __sys_setsockopt from ret_fast_syscall+0x0/0x5 This trace occurs because vlan_for_each() is called within cpsw_ndo_set_rx_mode(), which expects the RTNL lock to be held. Since modifying vlan_for_each() to operate without the RTNL lock is not straightforward, and because ndo_set_rx_mode() is invoked both with and without the RTNL lock across different code paths, simply adding rtnl_lock() in cpsw_ndo_set_rx_mode() is not a viable solution. To resolve this issue, we opt to execute the actual processing within a work queue, following the approach used by the icssg-prueth driver.	N/A	More Details
CVE-2026-23207	In the Linux kernel, the following vulnerability has been resolved: spi: tegra210-quad: Protect curr_xfer check in IRQ handler Now that all other accesses to curr_xfer are done under the lock, protect the curr_xfer NULL check in tegra_qspi_isr_thread() with the spinlock. Without this protection, the following race can occur: CPU0 (ISR thread) CPU1 (timeout path) ---------- ---------- if (!tqspi->curr_xfer) // sees non-NULL spin_lock() tqspi->curr_xfer = NULL spin_unlock() handle_*_xfer() spin_lock() t = tqspi->curr_xfer // NULL! ... t->len ... // NULL dereference! With this patch, all curr_xfer accesses are now properly synchronized. Although all accesses to curr_xfer are done under the lock, in tegra_qspi_isr_thread() it checks for NULL, releases the lock and reacquires it later in handle_cpu_based_xfer()/handle_dma_based_xfer(). There is a potential for an update in between, which could cause a NULL pointer dereference. To handle this, add a NULL check inside the handlers after acquiring the lock. This ensures that if the timeout path has already cleared curr_xfer, the handler will safely return without dereferencing the NULL pointer.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: smb/client: fix memory leak in smb2_open_file() Reproducer: 1. server: directories are exported read-only 2. client: mount -t cifs //${server_ip}/export /mnt 3. client: dd if=/dev/zero		

CVE-2026-23205	of=/mnt/file bs=512 count=1000 oflag=direct 4. client: umount /mnt 5. client: sleep 1 6. client: modprobe -r cifs The error message is as follows: == BUG cifs_small_rq (Not tainted): Objects remaining on __kmem_cache_shutdown() ---------- Object 0x00000000d47521be @offset=14336 ... WARNING: mm/slub.c:1251 at __kmem_cache_shutdown+0x34e/0x440, CPU#0: modprobe/1577 ... Call Trace: <TASK> kmem_cache_destroy+0x94/0x190 cifs_destroy_request_bufs+0x3e/0x50 [cifs] cleanup_module+0x4e/0x540 [cifs] __se_sys_delete_module+0x278/0x400 __x64_sys_delete_module+0x5f/0x70 x64_sys_call+0x2299/0x2ff0 do_syscall_64+0x89/0x350 entry_SYSCALL_64_after_hwframe+0x76/0x7e ... kmem_cache_destroy cifs_small_rq: Slab cache still has objects when called from cifs_destroy_request_bufs+0x3e/0x50 [cifs] WARNING: mm/slab_common.c:532 at kmem_cache_destroy+0x16b/0x190, CPU#0: modprobe/1577	N/A	More Details
CVE-2025-66614	Improper Input Validation vulnerability. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.14, from 10.1.0-M1 through 10.1.49, from 9.0.0-M1 through 9.0.112. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 through 8.5.100. Older EOL versions are not affected. Tomcat did not validate that the host name provided via the SNI extension was the same as the host name provided in the HTTP host header field. If Tomcat was configured with more than one virtual host and the TLS configuration for one of those hosts did not require client certificate authentication but another one did, it was possible for a client to bypass the client certificate authentication by sending different host names in the SNI extension and the HTTP host header field. The vulnerability only applies if client certificate authentication is only enforced at the Connector. It does not apply if client certificate authentication is enforced at the web application. Users are recommended to upgrade to version 11.0.15 or later, 10.1.50 or later or 9.0.113 or later, which fix the issue.	N/A	More Details
CVE-2025-32355	Rocket TRUfusion Enterprise through 7.10.4.0 uses a reverse proxy to handle incoming connections. However, the proxy is misconfigured in a way that allows specifying absolute URLs in the HTTP request line, causing the proxy to load the given resource.	N/A	More Details
CVE-2025-71221	In the Linux kernel, the following vulnerability has been resolved: dmaengine: mmp_pdma: Fix race condition in mmp_pdma_residue() Add proper locking in mmp_pdma_residue() to prevent use-after-free when accessing descriptor list and descriptor contents. The race occurs when multiple threads call tx_status() while the tasklet on another CPU is freeing completed descriptors: CPU 0 CPU 1 ----- ----- mmp_pdma_tx_status() mmp_pdma_residue() -> NO LOCK held list_for_each_entry(sw, ..) DMA interrupt dma_do_tasklet() -> spin_lock(&desc_lock) list_move(sw->node, ...) spin_unlock(&desc_lock) | dma_pool_free(sw) <- FREED! -> access sw->desc <- UAF! This issue can be reproduced when running dmatest on the same channel with multiple threads (threads_per_chan > 1). Fix by protecting the chain_running list iteration and descriptor access with the chan->desc_lock spinlock.	N/A	More Details
CVE-2025-59903	Stored Cross-Site Scripting (XSS) vulnerability in Kubysoft, where uploaded SVG images are not properly sanitized. This allows attackers to embed malicious scripts within SVG files as visual content, which are then stored on the server and executed in the context of any user accessing the compromised resource.	N/A	More Details
CVE-2025-59904	Stored Cross-Site Scripting (XSS) vulnerability in Kubysoft, which is triggered through multiple parameters in the '/kForms/app' endpoint. This issue allows malicious scripts to be injected and executed persistently in the context of users accessing the affected resource.	N/A	More Details
CVE-2025-59905	Cross-Site Scripting (XSS) vulnerability reflected in Kubysoft, which occurs through multiple parameters within the endpoint '/node/kudaby/nodeFN/procedure'. This flaw allows the injection of arbitrary client-side scripts, which are immediately reflected in the HTTP response and executed in the victim's browser.	N/A	More Details
CVE-2026-2415	Emails sent by pretix can utilize placeholders that will be filled with customer data. For example, when {name} is used in an email template, it will be replaced with the buyer's name for the final email. This mechanism contained two security-relevant bugs: * It was possible to exfiltrate information about the pretix system through specially crafted placeholder names such as {{event.__init__.__code__.co_filename}}. This way, an attacker with the ability to control email templates (usually every user of the pretix backend) could retrieve sensitive information from the system configuration, including even database passwords or API keys. pretix does include mechanisms to prevent the usage of such malicious placeholders, however due to a mistake in the code, they were not fully effective for the email subject. * Placeholders in subjects and plain text bodies of emails were wrongfully evaluated twice. Therefore, if the first evaluation of a placeholder again contains a placeholder, this second placeholder was rendered. This allows the rendering of placeholders controlled by the ticket buyer, and therefore the exploitation of the first issue as a ticket buyer. Luckily, the only buyer-controlled placeholder available in pretix by default (that is not validated in a way that prevents the issue) is {invoice_company}, which is very unusual (but not impossible) to be contained in an email subject template. In addition to broadening the attack surface of the first issue, this could theoretically also leak information about an order to one of the attendees within that order. However, we also consider this scenario very unlikely under typical conditions. Out of caution, we recommend that you rotate all passwords and API keys contained in your pretix.cfg https://docs.pretix.eu/self-hosting/config/ file.	N/A	More Details
CVE-2026-2451	Emails sent by pretix can utilize placeholders that will be filled with customer data. For example, when {name} is used in an email template, it will be replaced with the buyer's name for the final email. This mechanism contained a security-relevant bug: It was possible to exfiltrate information about the pretix system through specially crafted placeholder names such as {{event.__init__.__code__.co_filename}}. This way, an attacker with the ability to control email templates (usually every user of the pretix backend) could retrieve sensitive information from the system configuration, including even database passwords or API keys. pretix does include mechanisms to prevent the usage of such malicious placeholders, however due to a mistake in the code, they were not fully effective for this plugin. Out of caution, we recommend that you rotate all passwords and API keys contained in your pretix.cfg file.	N/A	More Details
CVE-2026-2452	Emails sent by pretix can utilize placeholders that will be filled with customer data. For example, when {name} is used in an email template, it will be replaced with the buyer's name for the final email. This mechanism contained a security-relevant bug: It was possible to exfiltrate information about the pretix system through specially crafted placeholder names such as {{event.__init__.__code__.co_filename}}. This way, an attacker with the ability to control email templates (usually every user of the pretix backend) could retrieve sensitive information from the system configuration, including even database passwords or API keys. pretix does include mechanisms to prevent the usage of such malicious placeholders, however due to a mistake in the code, they were not fully effective for this plugin. Out of caution, we recommend that you rotate all passwords and API keys contained in your pretix.cfg https://docs.pretix.eu/self-hosting/config/ file.	N/A	More Details

CVE-2026-26736	TOTOLINK A3002RU_V3 V3.0.0-B20220304.1804 was discovered to contain a stack-based buffer overflow via the static_ipv6 parameter in the formIpv6Setup function.	N/A	More Details
CVE-2026-26732	TOTOLINK A3002RU V2.1.1-B20211108.1455 was discovered to contain a stack-based buffer overflow via the vpnUser or vpnPassword` parameters in the formFilter function.	N/A	More Details
CVE-2026-26731	TOTOLINK A3002RU V2.1.1-B20211108.1455 was discovered to contain a stack-based buffer overflow via the routernamer`parameter in the formDnsv6 function.	N/A	More Details
CVE-2026-24734	Improper Input Validation vulnerability in Apache Tomcat Native, Apache Tomcat. When using an OCSP responder, Tomcat Native (and Tomcat's FFM port of the Tomcat Native code) did not complete verification or freshness checks on the OCSP response which could allow certificate revocation to be bypassed. This issue affects Apache Tomcat Native: from 1.3.0 through 1.3.4, from 2.0.0 through 2.0.11; Apache Tomcat: from 11.0.0-M1 through 11.0.17, from 10.1.0-M7 through 10.1.51, from 9.0.83 through 9.0.114. The following versions were EOL at the time the CVE was created but are known to be affected: from 1.1.23 through 1.1.34, from 1.2.0 through 1.2.39. Older EOL versions are not affected. Apache Tomcat Native users are recommended to upgrade to versions 1.3.5 or later or 2.0.12 or later, which fix the issue. Apache Tomcat users are recommended to upgrade to versions 11.0.18 or later, 10.1.52 or later or 9.0.115 or later which fix the issue.	N/A	More Details
CVE-2026-24733	Improper Input Validation vulnerability in Apache Tomcat. Tomcat did not limit HTTP/0.9 requests to the GET method. If a security constraint was configured to allow HEAD requests to a URI but deny GET requests, the user could bypass that constraint on GET requests by sending a (specification invalid) HEAD request using HTTP/0.9. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.14, from 10.1.0-M1 through 10.1.49, from 9.0.0.M1 through 9.0.112. Older, EOL versions are also affected. Users are recommended to upgrade to version 11.0.15 or later, 10.1.50 or later or 9.0.113 or later, which fixes the issue.	N/A	More Details
CVE-2025-65715	An issue in the code-runner.executorMap setting of Visual Studio Code Extensions Code Runner v0.12.2 allows attackers to execute arbitrary code when opening a crafted workspace.	N/A	More Details
CVE-2026-1783	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-2026-23206	In the Linux kernel, the following vulnerability has been resolved: dpaa2-switch: prevent ZERO_SIZE_PTR dereference when num_ifs is zero The driver allocates arrays for ports, FDBs, and filter blocks using kcalloc() with ethsw->sw_attr.num_ifs as the element count. When the device reports zero interfaces (either due to hardware configuration or firmware issues), kcalloc(0, ...) returns ZERO_SIZE_PTR (0x10) instead of NULL. Later in dpaa2_switch_probe(), the NAPI initialization unconditionally accesses ethsw->ports[0]->netdev, which attempts to dereference ZERO_SIZE_PTR (address 0x10), resulting in a kernel panic. Add a check to ensure num_ifs is greater than zero after retrieving device attributes. This prevents the zero-sized allocations and subsequent invalid pointer dereference.	N/A	More Details
CVE-2025-59793	Rocket TRUfusion Enterprise through 7.10.5 exposes the endpoint at /axis2/services/WsPortalV6UpDwAxis2Impl to authenticated users to be able to upload files. However, the application doesn't properly sanitize the jobDirectory parameter, which allows path traversal sequences to be included. This allows writing files to arbitrary local filesystem locations and may subsequently lead to remote code execution.	N/A	More Details
CVE-2026-1452	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-67102	A SQL injection vulnerability in the alldayoffs feature in Jorani up to v1.0.4, allows an authenticated attacker to execute arbitrary SQL commands via the entity parameter.	N/A	More Details
CVE-2025-70846	lty628 aidigu v1.9.1 is vulnerable to Cross Site Scripting (XSS) on the /tools/Password/add page in the input field password.	N/A	More Details
CVE-2026-2541	The Micca KE700 system relies on a 6-bit portion of an identifier for authentication within rolling codes, providing only 64 possible combinations. This low entropy allows an attacker to perform a brute-force attack against one component of the rolling code. Successful exploitation simplify an attacker to predict the next valid rolling code, granting unauthorized access to the vehicle.	N/A	More Details
CVE-2026-2540	The Micca KE700 system contains flawed resynchronization logic and is vulnerable to replay attacks. This attack requires sending two previously captured codes in a specific sequence. As a result, the system can be forced to accept previously used (stale) rolling codes and execute a command. Successful exploitation allows an attacker to clone the alarm key. This grants the attacker unauthorized access to the vehicle to unlock or lock the doors.	N/A	More Details
CVE-2026-2539	The RF communication protocol in the Micca KE700 car alarm system does not encrypt its data frames. An attacker with a radio interception tool (e.g., SDR) can capture the random number and counters transmitted in cleartext, which is sensitive information required for authentication.	N/A	More Details
CVE-2026-26220	LightLLM version 1.1.0 and prior contain an unauthenticated remote code execution vulnerability in PD (prefill-decode) disaggregation mode. The PD master node exposes WebSocket endpoints that receive binary frames and pass the data directly to pickle.loads() without authentication or validation. A remote attacker who can reach the PD master can send a crafted payload to achieve arbitrary code execution.	N/A	More Details
CVE-2025-	Pega Platform versions 8.1.0 through 25.1.1 are affected by a Stored Cross-site Scripting vulnerability in a user interface	N/A	More

62183	component. Requires an administrative user and given extensive access rights, impact to Confidentiality and Integrity are low.		Details
CVE-2026-25903	Apache NiFi 1.1.0 through 2.7.2 are missing authorization when updating configuration properties on extension components that have specific Required Permissions based on the Restricted annotation. The Restricted annotation indicates additional privileges required to add the annotated component to the flow configuration, but framework authorization did not check restricted status when updating a component previously added. The missing authorization requires a more privileged user to add a restricted component to the flow configuration, but permits a less privileged user to make property configuration changes. Apache NiFi installations that do not implement different levels of authorization for Restricted components are not subject to this vulnerability because the framework enforces write permissions as the security boundary. Upgrading to Apache NiFi 2.8.0 is the recommended mitigation.	N/A	More Details
CVE-2026-2247	SQL injection vulnerability (SQLi) in Clicldeu SaaS, specifically in the generation of reports, which occurs when a previously authenticated remote attacker executes a malicious payload in the URL generated after downloading the student's report card in the 'Day-to-day' section from the mobile application. In the URL of the generated PDF, the session token used does not expire, so it remains valid for days after its generation, and unusual characters can be entered after the 'id_alu' parameter, resulting in two types of SQLi: boolean-based blind and time-based blind. Exploiting this vulnerability could allow an attacker to access confidential information in the database.	N/A	More Details
CVE-2026-23210	In the Linux kernel, the following vulnerability has been resolved: ice: Fix PTP NULL pointer dereference during VSI rebuild Fix race condition where PTP periodic work runs while VSI is being rebuilt, accessing NULL vsi->rx_rings. The sequence was: 1. ice_ptp_prepare_for_reset() cancels PTP work 2. ice_ptp_rebuild() immediately queues PTP work 3. VSI rebuild happens AFTER ice_ptp_rebuild() 4. PTP work runs and accesses NULL vsi->rx_rings Fix: Keep PTP work cancelled during rebuild, only queue it after VSI rebuild completes in ice_rebuild(). Added ice_ptp_queue_work() helper function to encapsulate the logic for queuing PTP work, ensuring it's only queued when PTP is supported and the state is ICE_PTP_READY. Error log: [121.392544] ice 0000:60:00.1: PTP reset successful [121.392692] BUG: kernel NULL pointer dereference, address: 0000000000000000 [121.392712] #PF: supervisor read access in kernel mode [121.392720] #PF: error_code(0x0000) - not-present page [121.392727] PGD 0 [121.392734] Oops: Oops: 0000 [#1] SMP NOPTI [121.392746] CPU: 8 UID: 0 PID: 1005 Comm: ice-ptp-0000:60 Tainted: G S 6.19.0-rc6+ #4 PREEMPT(voluntary) [121.392761] Tainted: [S]=CPU_OUT_OF_SPEC [121.392773] RIP: 0010:ice_ptp_update_cached_phctime+0xbf/0x150 [ice] [121.393042] Call Trace: [121.393047] <TASK> [121.393055] ice_ptp_periodic_work+0x69/0x180 [ice] [121.393202] kthread_worker_fn+0xa2/0x260 [121.393216] ? __pfx_ice_ptp_periodic_work+0x10/0x10 [ice] [121.393359] ? __pfx_kthread_worker_fn+0x10/0x10 [121.393371] kthread+0x10d/0x230 [121.393382] ? __pfx_kthread+0x10/0x10 [121.393393] ret_from_fork+0x273/0x2b0 [121.393407] ? __pfx_kthread+0x10/0x10 [121.393417] ret_from_fork_asm+0x1a/0x30 [121.393432] </TASK>	N/A	More Details
CVE-2026-23209	In the Linux kernel, the following vulnerability has been resolved: macvlan: fix error recovery in macvlan_common_newlink() valis provided a nice repro to crash the kernel: ip link add p1 type veth peer p2 ip link set address 00:00:00:00:00:20 dev p1 ip link set up dev p1 ip link set up dev p2 ip link add mv0 link p2 type macvlan mode source ip link add invalid% link p2 type macvlan mode source macaddr add 00:00:00:00:00:20 ping -c1 -I p1 1.2.3.4 He also gave a very detailed analysis: <quote valis> The issue is triggered when a new macvlan link is created with MACVLAN_MODE_SOURCE mode and MACVLAN_MACADDR_ADD (or MACVLAN_MACADDR_SET) parameter, lower device already has a macvlan port and register_netdevice() called from macvlan_common_newlink() fails (e.g. because of the invalid link name). In this case macvlan_hash_add_source is called from macvlan_change_sources() / macvlan_common_newlink(): This adds a reference to vlan to the port's vlan_source_hash using macvlan_source_entry. vlan is a pointer to the priv data of the link that is being created. When register_netdevice() fails, the error is returned from macvlan_newlink() to rtnl_newlink_create(): if (ops->newlink) err = ops->newlink(dev, &params, extack); else err = register_netdevice(dev); if (err < 0) { free_netdev(dev); goto out; } and free_netdev() is called, causing a kvfree() on the struct net_device that is still referenced in the source entry attached to the lower device's macvlan port. Now all packets sent on the macvlan port with a matching source mac address will trigger a use-after-free in macvlan_forward_source(). </quote valis> With all that, my fix is to make sure we call macvlan_flush_sources() regardless of @create value whenever "goto destroy_macvlan_port;" path is taken. Many thanks to valis for following up on this issue.	N/A	More Details
CVE-2026-23208	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Prevent excessive number of frames In this case, the user constructed the parameters with maxpacksize 40 for rate 22050 / pps 1000, and packsize[0] 22 packsize[1] 23. The buffer size for each data URB is maxpacksize * packets, which in this example is 40 * 6 = 240; When the user performs a write operation to send audio data into the ALSA PCM playback stream, the calculated number of frames is packsize[0] * packets = 264, which exceeds the allocated URB buffer size, triggering the out-of-bounds (OOB) issue reported by syzbot [1]. Added a check for the number of single data URB frames when calculating the number of frames to prevent [1]. [1] BUG: KASAN: slab-out-of-bounds in copy_to_urb+0x261/0x460 sound/usb/pcm.c:1487 Write of size 264 at addr ffff88804337e800 by task syz.0.17/5506 Call Trace: copy_to_urb+0x261/0x460 sound/usb/pcm.c:1487 prepare_playback_urb+0x953/0x13d0 sound/usb/pcm.c:1611 prepare_outbound_urb+0x377/0xc50 sound/usb/endpoint.c:333	N/A	More Details
CVE-2025-71222	In the Linux kernel, the following vulnerability has been resolved: wifi: wlcore: ensure skb headroom before skb_push This avoids occasional skb_under_panic Oops from wl1271_tx_work. In this case, headroom is less than needed (typically 110 - 94 = 16 bytes).	N/A	More Details
CVE-2026-1571	User-controlled input is reflected into the HTML output without proper encoding on TP-Link Archer C60 v3, allowing arbitrary JavaScript execution via a crafted URL. An attacker could run script in the device web UI context, potentially enabling credential theft, session hijacking, or unintended actions if a privileged user is targeted.	N/A	More Details
CVE-2025-71220	In the Linux kernel, the following vulnerability has been resolved: smb/server: call ksmbd_session_rpc_close() on error path in create_smb2_pipe() When ksmbd_iov_pin_rsp() fails, we should call ksmbd_session_rpc_close().	N/A	More Details
CVE-2026-25768	LavinMQ is a high-performance message queue & streaming server. Before 2.6.6, an authenticated user could access metadata in the broker they should not have access to. This vulnerability is fixed in 2.6.6.	N/A	More Details
CVE-2025-48020	A vulnerability has been found in Vnet/IP Interface Package provided by Yokogawa Electric Corporation. If affected product receives maliciously crafted packets, Vnet/IP software stack process may be terminated. The affected products and versions are as follows: Vnet/IP Interface Package (for CENTUM VP R6 VP6C3300, CENTUM VP R7 VP7C3300) R1.07.00 or earlier	N/A	More Details

CVE-2025-48019	A vulnerability has been found in Vnet/IP Interface Package provided by Yokogawa Electric Corporation. If affected product receives maliciously crafted packets, Vnet/IP software stack process may be terminated. The affected products and versions are as follows: Vnet/IP Interface Package (for CENTUM VP R6 VP6C3300, CENTUM VP R7 VP7C3300) R1.07.00 or earlier	N/A	More Details
CVE-2025-1924	A vulnerability has been found in Vnet/IP Interface Package provided by Yokogawa Electric Corporation. If affected product receive maliciously crafted packets, a DoS attack may cause Vnet/IP communication functions to stop or arbitrary programs to be executed. The affected products and versions are as follows: Vnet/IP Interface Package (for CENTUM VP R6 VP6C3300, CENTUM VP R7 VP7C3300) R1.07.00 or earlier	N/A	More Details
CVE-2026-26257	Rejected reason: Not used	N/A	More Details
CVE-2026-26256	Rejected reason: Not used	N/A	More Details
CVE-2026-26255	Rejected reason: Not used	N/A	More Details
CVE-2026-26254	Rejected reason: Not used	N/A	More Details
CVE-2026-26253	Rejected reason: Not used	N/A	More Details
CVE-2026-26252	Rejected reason: Not used	N/A	More Details
CVE-2026-26251	Rejected reason: Not used	N/A	More Details
CVE-2026-26250	Rejected reason: Not used	N/A	More Details
CVE-2026-26249	Rejected reason: Not used	N/A	More Details
CVE-2026-25108	FileZen contains an OS command injection vulnerability. When FileZen Antivirus Check Option is enabled, a logged-in user may send a specially crafted HTTP request to execute an arbitrary OS command.	N/A	More Details
CVE-2026-1721	Summary A Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the AI Playground's OAuth callback handler. The `error_description` query parameter was directly interpolated into an HTML script tag without proper escaping, allowing attackers to execute arbitrary JavaScript in the context of the victim's session. Root cause The OAuth callback handler in `site/ai-playground/src/server.ts` directly interpolated the `authError` value, sourced from the `error_description` query parameter, into an inline `<script>` tag. Impact An attacker could craft a malicious link that, when clicked by a victim, would: * Steal user chat message history - Access all LLM interactions stored in the user's session. * Access connected MCP Servers - Interact with any MCP servers connected to the victim's session (public or authenticated/private), potentially allowing the attacker to perform actions on the victim's behalf Mitigation: * PR: https://github.com/cloudflare/agents/pull/841 https://github.com/cloudflare/agents/pull/841 * Agents-sdk users should upgrade to agents@0.3.10 * Developers using configureOAuthCallback with custom error handling in their own applications should ensure all user-controlled input is escaped before interpolation.	N/A	More Details
CVE-2025-9293	A vulnerability in the certificate validation logic may allow applications to accept untrusted or improperly validated server identities during TLS communication. An attacker in a privileged network position may be able to intercept or modify traffic if they can position themselves within the communication channel. Successful exploitation may compromise confidentiality, integrity, and availability of application data.	N/A	More Details
CVE-2025-9292	A permissive web security configuration may allow cross-origin restrictions enforced by modern browsers to be bypassed under specific circumstances. Exploitation requires the presence of an existing client-side injection vulnerability and user access to the affected web interface. Successful exploitation could allow unauthorized disclosure of sensitive information. Fixed in updated Omada Cloud Controller service versions deployed automatically by TP-Link. No user action is required.	N/A	More Details
CVE-2024-21961	Improper restriction of operations within the bounds of a memory buffer in PCIe® Link could allow an attacker with access to a guest virtual machine to potentially perform a denial of service attack against the host resulting in loss of availability.	N/A	More Details
CVE-2026-26188	Solspace Freeform plugin for Craft CMS 5.x is a super flexible form-building tool. An authenticated, low-privilege user (able to create/edit forms) can inject arbitrary HTML/JS into the Craft Control Panel (CP) builder and integrations views. User-controlled form labels and integration metadata are rendered with dangerouslySetInnerHTML without sanitization, leading to stored XSS that executes when any admin views the builder/integration screens. This vulnerability is fixed in 5.14.7.	N/A	More Details
CVE-2026-	Intego Personal Backup, a macOS backup utility that allows users to create scheduled backups and bootable system clones, contains a local privilege escalation vulnerability. Backup task definitions are stored in a location writable by non-privileged	N/A	More

26225	users while being processed with elevated privileges. By crafting a malicious serialized task file, a local attacker can trigger arbitrary file writes to sensitive system locations, leading to privilege escalation to root.		Details
CVE-2026-26224	Intego Log Reporter, a macOS diagnostic utility bundled with Intego security products that collects system and application logs for support analysis, contains a local privilege escalation vulnerability. A root-executed diagnostic script creates and writes files in /tmp without enforcing secure directory handling, introducing a time-of-check to time-of-use (TOCTOU) race condition. A local unprivileged user can exploit a symlink-based race condition to cause arbitrary file writes to privileged system locations, resulting in privilege escalation to root.	N/A	More Details
CVE-2026-26076	ntpd-rs is a full-featured implementation of the Network Time Protocol. Prior to 1.7.1, an attacker can remotely induce moderate increases (2-4 times above normal) in cpu usage. When having NTS enabled on an ntpd-rs server, an attacker can create malformed NTS packets that take significantly more effort for the server to respond to by requesting a large number of cookies. This can lead to degraded server performance even when a server could otherwise handle the load. This vulnerability is fixed in 1.7.1.	N/A	More Details
CVE-2026-26075	FastGPT is an AI Agent building platform. Due to the fact that FastGPT's web page acquisition nodes, HTTP nodes, etc. need to initiate data acquisition requests from the server, there are certain security issues. In addition to implementing internal network isolation in the deployment environment, this optimization has added stricter internal network address detection. This vulnerability is fixed in 4.14.7.	N/A	More Details
CVE-2026-26069	Scraparr is a Prometheus Exporter for various components of the *arr Suite. From 3.0.0-beta to before 3.0.2, when the Readarr integration was enabled, the exporter exposed the configured Readarr API key as the alias metric label value. Users were affected only if all of the following conditions are met, Readarr scraping feature was enabled and no alias configured, the exporter’s /metrics endpoint was accessible to external or unauthorized users, and the Readarr instance is externally accessible. If the /metrics endpoint was publicly accessible, the Readarr API key could have been disclosed via exported metrics data. This vulnerability is fixed in 3.0.2.	N/A	More Details
CVE-2026-26068	emp3r0r is a stealth-focused C2 designed by Linux users for Linux environments. Prior to 3.21.1, untrusted agent metadata (Transport, Hostname) is accepted during check-in and later interpolated into tmux shell command strings executed via /bin/sh -c. This enables command injection and remote code execution on the operator host. This vulnerability is fixed in 3.21.1.	N/A	More Details
CVE-2026-26011	navigation2 is a ROS 2 Navigation Framework and System. In 1.3.11 and earlier, a critical heap out-of-bounds write vulnerability exists in Nav2 AMCL's particle filter clustering logic. By publishing a single crafted geometry_msgs/PoseWithCovarianceStamped message with extreme covariance values to the /initialpose topic, an unauthenticated attacker on the same ROS 2 DDS domain can trigger a negative index write (set->clusters[-1]) into heap memory preceding the allocated buffer. In Release builds, the sole boundary check (assert) is compiled out, leaving zero runtime protection. This primitive allows controlled corruption of the heap chunk metadata(at least the size of the heap chunk where the set->clusters is in is controllable by the attacker), potentially leading to further exploitation. At minimum, it provides a reliable single-packet denial of service that kills localization and halts all navigation.	N/A	More Details
CVE-2026-26000	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Prior to 17.9.0, 17.4.6, and 16.10.13, it's possible using comments to inject CSS that would transform the full wiki in a link area leading to a malicious page. This vulnerability is fixed in 17.9.0, 17.4.6, and 16.10.13.	N/A	More Details
CVE-2026-25996	Inspektor Gadget is a set of tools and framework for data collection and system inspection on Kubernetes clusters and Linux hosts using eBPF. String fields from eBPF events in columns output mode are rendered to the terminal without any sanitization of control characters or ANSI escape sequences. Therefore, a maliciously forged – partially or completely – event payload, coming from an observed container, might inject the escape sequences into the terminal of ig operators, with various effects. The columns output mode is the default when running ig run interactively.	N/A	More Details
CVE-2025-48021	A vulnerability has been found in Vnet/IP Interface Package provided by Yokogawa Electric Corporation. If affected product receives maliciously crafted packets, Vnet/IP software stack process may be terminated. The affected products and versions are as follows: Vnet/IP Interface Package (for CENTUM VP R6 VP6C3300, CENTUM VP R7 VP7C3300) R1.07.00 or earlier	N/A	More Details
CVE-2025-48022	A vulnerability has been found in Vnet/IP Interface Package provided by Yokogawa Electric Corporation. If affected product receives maliciously crafted packets, Vnet/IP software stack process may be terminated. The affected products and versions are as follows: Vnet/IP Interface Package (for CENTUM VP R6 VP6C3300, CENTUM VP R7 VP7C3300) R1.07.00 or earlier	N/A	More Details
CVE-2025-48023	A vulnerability has been found in Vnet/IP Interface Package provided by Yokogawa Electric Corporation. If affected product receives maliciously crafted packets, Vnet/IP software stack process may be terminated. The affected products and versions are as follows: Vnet/IP Interface Package (for CENTUM VP R6 VP6C3300, CENTUM VP R7 VP7C3300) R1.07.00 or earlier	N/A	More Details
CVE-2025-20110	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-27928	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-27573	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-27569	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-27251	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2025-26471	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-25049	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-24524	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-24518	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-24492	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-24321	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-24300	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-22845	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-20107	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-0872	Improper Certificate Validation vulnerability in Thales SafeNet Agent for Windows Logon on Windows allows Signature Spoofing by Improper Validation.This issue affects SafeNet Agent for Windows Logon: 4.0.0, 4.1.1, 4.1.2.	N/A	More Details
CVE-2025-20098	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-20089	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-20078	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-20066	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-20038	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-20007	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-26226	beautiful-mermaid versions prior to 0.1.3 contain an SVG attribute injection issue that can lead to cross-site scripting (XSS) when rendering attacker-controlled Mermaid diagrams. User-controlled values from Mermaid style and classDef directives are interpolated into SVG attribute values without proper escaping, allowing crafted input to break out of an attribute context and inject arbitrary SVG elements/attributes into the rendered output. When the generated SVG is embedded in a web page, this can result in script execution in the context of the embedding origin.	N/A	More Details
CVE-2025-1790	Local privilege escalation in Genetec Sipelia Plugin. An authenticated low-privileged Windows user could exploit this vulnerability to gain elevated privileges on the affected system.	N/A	More Details
CVE-2026-26221	Hyland OnBase contains an unauthenticated .NET Remoting exposure in the OnBase Workflow Timer Service (Hyland.Core.Workflow.NTService.exe). An attacker who can reach the service can send crafted .NET Remoting requests to default HTTP channel endpoints on TCP/8900 (e.g., TimerServiceAPI.rem and TimerServiceEvents.rem for Workflow) to trigger unsafe object unmarshalling, enabling arbitrary file read/write. By writing attacker-controlled content into web-accessible locations or chaining with other OnBase features, this can lead to remote code execution. The same primitive can be abused by supplying a UNC path to coerce outbound NTLM authentication (SMB coercion) to an attacker-controlled host.	N/A	More Details
CVE-			

2026-1578	HP App for Android is potentially vulnerable to cross-site scripting (XSS) when using an outdated version of the application via mobile devices. HP is releasing updates to mitigate these potential vulnerabilities.	N/A	More Details
CVE-2026-23112	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: add bounds checks in nvmet_tcp_build_pdu_iovec nvmet_tcp_build_pdu_iovec() could walk past cmd->req.sg when a PDU length or offset exceeds sg_cnt and then use bogus sg->length/offset values, leading to _copy_to_iter() GPF/KASAN. Guard sg_idx, remaining entries, and sg->length/offset before building the bvec.	N/A	More Details
CVE-2026-23111	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix inverted genmask check in nft_map_catchall_activate() nft_map_catchall_activate() has an inverted element activity check compared to its non-catchall counterpart nft_mapelem_activate() and compared to what is logically required. nft_map_catchall_activate() is called from the abort path to re-activate catchall map elements that were deactivated during a failed transaction. It should skip elements that are already active (they don't need re-activation) and process elements that are inactive (they need to be restored). Instead, the current code does the opposite: it skips inactive elements and processes active ones. Compare the non-catchall activate callback, which is correct: nft_mapelem_activate(): if (nft_set_elem_active(ext, iter->genmask)) return 0; /* skip active, process inactive */ With the buggy catchall version: nft_map_catchall_activate(): if (!nft_set_elem_active(ext, genmask)) continue; /* skip inactive, process active */ The consequence is that when a DELSET operation is aborted, nft_setelem_data_activate() is never called for the catchall element. For NFT_GOTO verdict elements, this means nft_data_hold() is never called to restore the chain->use reference count. Each abort cycle permanently decrements chain->use. Once chain->use reaches zero, DELCHAIN succeeds and frees the chain while catchall verdict elements still reference it, resulting in a use-after-free. This is exploitable for local privilege escalation from an unprivileged user via user namespaces + nftables on distributions that enable CONFIG_USER_NS and CONFIG_NF_TABLES. Fix by removing the negation so the check matches nft_mapelem_activate(): skip active elements, process inactive ones.	N/A	More Details
CVE-2026-0619	A reachable infinite loop via an integer wraparound is present in Silicon Labs' Matter SDK which allows an attacker to trigger a denial of service. A hard reset is required to recover the device.	N/A	More Details
CVE-2026-25767	LavinMQ is a high-performance message queue & streaming server. Before 2.6.8, an authenticated user, with the “Policymaker” tag, could create shovels bypassing access controls. an authenticated user with the "Policymaker" management tag could exploit it to read messages from vhosts they are not authorized to access or publish messages to vhosts they are not authorized to access. This vulnerability is fixed in 2.6.8.	N/A	More Details
CVE-2025-71204	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix refcount leak in parse_durable_handle_context() When the command is a replay operation and -ENOEXEC is returned, the refcount of ksmbd_file must be released.	N/A	More Details
CVE-2026-24895	FrankenPHP is a modern application server for PHP. Prior to 1.11.2, FrankenPHP’s CGI path splitting logic improperly handles Unicode characters during case conversion. The logic computes the split index (for finding .php) on a lowercased copy of the request path but applies that byte index to the original path. Because strings.ToLower() in Go can increase the byte length of certain UTF-8 characters (e.g., Ⱥ expands when lowercased), the computed index may not align with the correct position in the original string. This results in an incorrect SCRIPT_NAME and SCRIPT_FILENAME, potentially causing FrankenPHP to execute a file other than the one intended by the URI. This vulnerability is fixed in 1.11.2.	N/A	More Details
CVE-2026-25868	MiniGal Nano version 0.3.5 and prior contain a reflected cross-site scripting (XSS) vulnerability in index.php via the dir parameter. The application constructs $currentdir from user-controlled input and embeds it into an error message without output encoding, allowing an attacker to supply HTML/JavaScript that is reflected in the response. Successful exploitation can lead to execution of arbitrary script in a victim's browser in the context of the vulnerable application.	N/A	More Details
CVE-2026-1837	A specially-crafted file can cause libjxl's decoder to write pixel data to uninitialized unallocated memory. Soon after that data from another uninitialized unallocated region is copied to pixel data. This can be done by requesting color transformation of grayscale images to another grayscale color space. Buffers allocated for 1-float-per-pixel are used as if they are allocated for 3-float-per-pixel. That happens only if LCMS2 is used as CMS engine. There is another CMS engine available (selected by build flags).	N/A	More Details
CVE-2025-12474	A specially-crafted file can cause libjxl's decoder to read pixel data from uninitialized (but allocated) memory. This can be done by causing the decoder to reference an outside-image-bound area in a subsequent patches. An incorrect optimization causes the decoder to omit populating those areas.	N/A	More Details
CVE-2026-2344	A vulnerability in Plunet Plunet BusinessManager allows unauthorized actions being performed on behalf of privileged users.This issue affects Plunet BusinessManager: 10.15.1	N/A	More Details
CVE-2025-61969	Incorrect permission assignment in AMD µProf may allow a local user-privileged attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2025-48518	Improper input validation in AMD Graphics Driver could allow a local attacker to write out of bounds, potentially resulting in loss of integrity or denial of service.	N/A	More Details
CVE-2024-36320	Integer Overflow within atihdwt6.sys can allow a local attacker to cause out of bound read/write potentially leading to loss of confidentiality, integrity and availability	N/A	More Details
CVE-2023-31324	A Time-of-check time-of-use (TOCTOU) race condition in the AMD Secure Processor (ASP) could allow an attacker to modify External Global Memory Interconnect Trusted Agent (XGMI TA) commands as they are processed potentially resulting in loss of confidentiality, integrity, or availability.	N/A	More Details
CVE-2023-20548	A Time-of-check time-of-use (TOCTOU) race condition in the AMD Secure Processor (ASP) could allow an attacker to corrupt memory resulting in loss of integrity, confidentiality, or availability.	N/A	More Details

CVE-2023-20514	Improper handling of parameters in the AMD Secure Processor (ASP) could allow a privileged attacker to pass an arbitrary memory value to functions in the trusted execution environment resulting in arbitrary code execution	N/A	More Details
CVE-2026-2337	A vulnerability in Plunet Plunet BusinessManager allows session hijacking, data theft, unauthorized actions on behalf of the user.This issue affects Plunet BusinessManager: 10.15.1.	N/A	More Details
CVE-2026-1227	CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause unauthorized disclosure of local files, interaction within the EBO system, or denial of service conditions when a local user uploads a specially crafted TGML graphics file to the EBO server from Workstation.	N/A	More Details
CVE-2026-1226	CWE-94: Improper Control of Generation of Code vulnerability exists that could cause execution of untrusted or unintended code within the application when maliciously crafted design content is processed through a TGML graphics file.	N/A	More Details
CVE-2025-47205	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.8.3332 build 20251128 and later QuTS hero h5.2.8.3321 build 20251117 and later	N/A	More Details
CVE-2025-13651	Exposure of Sensitive System Information to an Unauthorized Actor vulnerability in Microcom ZeusWeb allows Web Application Fingerprinting of sensitive data. This issue affects ZeusWeb: 6.1.31.	N/A	More Details
CVE-2025-13650	An attacker with access to the web application ZeusWeb of the provider Microcom (in this case, registration is not necessary, but the action must be performed) who has the vulnerable software could introduce arbitrary JavaScript by injecting an XSS payload into the ‘Surname’ parameter of the ‘Create Account’ operation at the URL: https://zeus.microcom.es:4040/index.html?zeus6=true . This issue affects ZeusWeb: 6.1.31.	N/A	More Details
CVE-2025-13649	An attacker with access to the web application ZeusWeb of the provider Microcom (in this case, registration is not necessary, but the action must be performed) who has the vulnerable software could introduce arbitrary JavaScript by injecting an XSS payload into the ‘Email’ parameters within the ‘Recover password’ section at the URL: https://zeus.microcom.es:4040/index.html?zeus6=true . This issue affects ZeusWeb: 6.1.31.	N/A	More Details
CVE-2025-13648	An attacker with access to the web application ZeusWeb of the provider Microcom (in this case, registration is required) who has the vulnerable software could introduce arbitrary JavaScript by injecting an XSS payload into the ‘Name’ and “Surname” parameters within the ‘My Account’ section at the URL: https://zeus.microcom.es:4040/administracion-estaciones.html resulting in a stored XSS. This issue affects ZeusWeb: 6.1.31.	N/A	More Details
CVE-2026-26044	Rejected reason: Not used	N/A	More Details
CVE-2026-26043	Rejected reason: Not used	N/A	More Details
CVE-2026-26042	Rejected reason: Not used	N/A	More Details
CVE-2026-26041	Rejected reason: Not used	N/A	More Details
CVE-2026-26040	Rejected reason: Not used	N/A	More Details
CVE-2026-26039	Rejected reason: Not used	N/A	More Details
CVE-2026-26038	Rejected reason: Not used	N/A	More Details
CVE-2026-26037	Rejected reason: Not used	N/A	More Details
CVE-2026-26036	Rejected reason: Not used	N/A	More Details
CVE-2026-25869	MiniGal Nano versions 0.3.5 and prior contain a path traversal vulnerability in index.php via the dir parameter. The application appends user-controlled input to the photos directory and attempts to prevent traversal by removing dot-dot sequences, but this protection can be bypassed using crafted directory patterns. An attacker can exploit this behavior to cause the application to enumerate and display image files from unintended filesystem locations that are readable by the web server, resulting in unintended information disclosure.	N/A	More Details

CVE-2026-0228	An improper certificate validation vulnerability in PAN-OS allows users to connect Terminal Server Agents on Windows to PAN-OS using expired certificates even if the PAN-OS configuration would not normally permit them to do so.	N/A	More Details
CVE-2026-0229	A denial-of-service (DoS) vulnerability in the Advanced DNS Security (ADNS) feature of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to initiate system reboots using a maliciously crafted packet. Repeated attempts to initiate a reboot causes the firewall to enter maintenance mode. Cloud NGFW and Prisma Access® are not impacted by this vulnerability.	N/A	More Details
CVE-2025-15577	An unauthenticated attacker can exploit this vulnerability by manipulating URL to achieve arbitrary file read access.This issue affects Valmet DNA Web Tools: C2022 and older.	N/A	More Details
CVE-2026-24894	FrankenPHP is a modern application server for PHP. Prior to 1.11.2, when running FrankenPHP in worker mode, the $_SESSION superglobal is not correctly reset between requests. This allows a subsequent request processed by the same worker to access the $_SESSION data of the previous request (potentially belonging to a different user) before session_start() is called. This vulnerability is fixed in 1.11.2.	N/A	More Details
CVE-2026-24044	Element Server Suite Community Edition (ESS Community) deploys a Matrix stack using the provided Helm charts and Kubernetes distribution. The ESS Community Helm Chart secrets initialization hook (using matrix-tools container before 0.5.7) is using an insecure Matrix server key generation method, allowing network attackers to potentially recreate the same key pair, allowing them to impersonate the victim server. The secret is generated by the secrets initialization hook, in the ESS Community Helm Chart values, if both initSecrets.enabled is not set to false and synapse.signingKey is not defined. Given a server key in Matrix authenticates both requests originating from and events constructed on a given server, this potentially impacts confidentiality, integrity and availability of rooms which have a vulnerable server present as a member. The confidentiality of past conversations in end-to-end encrypted rooms is not impacted. The key generation issue was fixed in matrix-tools 0.5.7, released as part of ESS Community Helm Chart 25.12.1.	N/A	More Details
CVE-2025-67433	A heap buffer overflow in the processRequest function of Open TFTP Server MultiThreaded v1.7 allows attackers to cause a Denial of Service (DoS) via a crafted DATA packet.	N/A	More Details
CVE-2019-25348	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-69806	p2r3 bareiron commit: 8e4d4020d contains an Out-of-bounds Read, which allows unauthenticated remote attackers to get relative information leakage via a packet sent to the server	N/A	More Details
CVE-2025-52533	Improper Access Control in an on-chip debug interface could allow a privileged attacker to enable a debug interface and potentially compromise data confidentiality or integrity.	N/A	More Details
CVE-2024-36319	Debug code left active in AMD's Video Decoder Engine Firmware (VCN FW) could allow a attacker to submit a maliciously crafted command causing the VCN FW to perform read/writes HW registers, potentially impacting confidentiality, integrity and availabilability of the system.	N/A	More Details
CVE-2023-31323	Type confusion in the AMD Secure Processor (ASP) could allow an attacker to pass a malformed argument to the External Global Memory Interconnect Trusted Agent (XGMI TA) leading to a memory safety violation potentially resulting in loss of confidentiality, integrity, or availability.	N/A	More Details
CVE-2023-20601	Improper input validation within RAS TA Driver can allow a local attacker to access out-of-bounds memory, potentially resulting in a denial-of-service condition.	N/A	More Details
CVE-2025-55210	FreePBX is an open-source web-based graphical user interface (GUI) that manages Asterisk. Prior to 17.0.5 and 16.0.17, FreePBX module api (PBX API) is vulnerable to privilege escalation by authenticated users with REST/GraphQL API access. This vulnerability allows an attacker to forge a valid JWT with full access to the REST and GraphQL APIs on a FreePBX that they've already connected to, possibly as a lower privileged user. The JWT is signed using the api-oauth.key private key. An attacker can generate their own token if they possess this key (e.g., by accessing an affected instance), and specify any scopes they wish (e.g., rest, gql), bypassing traditional authorization checks. However, FreePBX enforces that the jti (JWT ID) claim must exist in the database (api_access_tokens table in the asterisk MySQL database) in order for the token to be accepted. Therefore, the attacker must know a jti value that already exists on the target instance. This vulnerability is fixed in 17.0.5 and 16.0.17.	N/A	More Details
CVE-2025-69752	An issue in the "My Details" user profile functionality of Ideagen Q-Pulse 7.1.0.32 allows an authenticated user to view other users' profile information by modifying the objectKey HTTP parameter in the My Details page URL.	N/A	More Details
CVE-2026-2276	Reflected Cross-Site Scripting (XSS) vulnerability in the Wix web application, where the endpoint ' https://manage.wix.com/account/account-settings ', responsible for uploading SVG images, does not properly sanitize the content. An authenticated attacker could upload an SVG file containing embedded JavaScript code, which is stored and subsequently executed when other users view the image. Exploiting this vulnerability allows arbitrary code to be executed in the context of the victim's browser, which could lead to the disclosure of sensitive information or the abuse of the affected user's session.	N/A	More Details
CVE-2026-26092	Rejected reason: Not used	N/A	More Details
CVE-	Outline is a service that allows for collaborative documentation. Prior to 1.1.0, a vulnerability was found in Outline's WebSocket		

2025-68663	authentication mechanism that allows suspended users to maintain or establish real-time WebSocket connections and continue receiving sensitive operational updates after their account has been suspended. This vulnerability is fixed in 1.1.0.	N/A	More Details
CVE-2026-26091	Rejected reason: Not used	N/A	More Details
CVE-2026-26090	Rejected reason: Not used	N/A	More Details
CVE-2026-26089	Rejected reason: Not used	N/A	More Details
CVE-2026-26088	Rejected reason: Not used	N/A	More Details
CVE-2026-26087	Rejected reason: Not used	N/A	More Details
CVE-2026-26086	Rejected reason: Not used	N/A	More Details
CVE-2026-26085	Rejected reason: Not used	N/A	More Details
CVE-2026-25676	The installer of M-Track Duo HD version 1.0.0 contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with administrator privileges.	N/A	More Details
CVE-2026-26215	manga-image-translator version beta-0.3 and prior in shared API mode contains an unsafe deserialization vulnerability that can lead to unauthenticated remote code execution. The FastAPI endpoints /simple_execute/{method} and /execute/{method} deserialize attacker-controlled request bodies using pickle.loads() without validation. Although a nonce-based authorization check is intended to restrict access, the nonce defaults to an empty string and the check is skipped, allowing remote attackers to execute arbitrary code in the server context by sending a crafted pickle payload.	N/A	More Details
CVE-2026-1669	Arbitrary file read in the model loading mechanism (HDF5 integration) in Keras versions 3.0.0 through 3.13.1 on all supported platforms allows a remote attacker to read local files and disclose sensitive information via a crafted .keras model file utilizing HDF5 external dataset references.	N/A	More Details
CVE-2026-25994	PJSIP is a free and open source multimedia communication library written in C. In 2.16 and earlier, a buffer overflow vulnerability exists in PJNATH ICE Session when processing credentials with excessively long usernames.	N/A	More Details
CVE-2026-25935	Vikunja is a todo-app to organize your life. Prior to 1.1.0, TaskGlanceTooltip.vue temporarily creates a div and sets the innerHtml to the description. Since there is no escaping on either the server or client side, a malicious user can share a project, create a malicious task, and cause an XSS on hover. This vulnerability is fixed in 1.1.0.	N/A	More Details
CVE-2025-27941	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-29869	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-30517	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-31145	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-23144	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: cleanup attrs subdirs on context dir setup failure When a context DAMON sysfs directory setup is failed after setup of attrs/ directory, subdirectories of attrs/ directory are not cleaned up. As a result, DAMON sysfs interface is nearly broken until the system reboots, and the memory for the unremoved directory is leaked. Cleanup the directories under such failures.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: virtio_net: Fix misalignment bug in struct virtnet_info Use the new TRAILING_OVERLAP() helper to fix a misalignment bug along with the following warning: drivers/net/virtio_net.c:429:46: warning: structure containing a flexible array member is not at the end of another structure [-Wflex-array-member-not-at-end] This helper creates a union between a flexible-array member (FAM) and a set of members that would otherwise follow it (in this case `u8 rss_hash_key_data[VIRTIO_NET_RSS_MAX_KEY_SIZE];`). This overlays the trailing members (rss_hash_key_data) onto the FAM (hash_key_data) while keeping the FAM and the start of MEMBERS aligned. The static_assert() ensures this alignment remains. Notice that due to tail padding in flexible `struct virtio_net_rss_config_trailer`, `rss_trailer.hash_key_data` (at offset 83 in struct virtnet_info) and `rss_hash_key_data` (at offset 84 in struct virtnet_info) are misaligned by one byte. See below: struct		

CVE-2026-23143	virtio_net_rss_config_trailer { __le16 max_tx_vq; /* 0 2 */ __u8 hash_key_length; /* 2 1 */ __u8 hash_key_data[]; /* 3 0 */ /* size: 4, cachelines: 1, members: 3 */ /* padding: 1 */ /* last cacheline: 4 bytes */ }; struct virtnet_info { ... struct virtio_net_rss_config_trailer rss_trailer; /* 80 4 */ /* XXX last struct has 1 byte of padding */ u8 rss_hash_key_data[40]; /* 84 40 */ ... /* size: 832, cachelines: 13, members: 48 */ /* sum members: 801, holes: 8, sum holes: 31 */ /* paddings: 2, sum paddings: 5 */ }; After changes, those members are correctly aligned at offset 795: struct virtnet_info { ... union { struct virtio_net_rss_config_trailer rss_trailer; /* 792 4 */ struct { unsigned char __offset_to_hash_key_data[3]; /* 792 3 */ u8 rss_hash_key_data[40]; /* 795 40 */ }; /* 792 43 */ }; /* 792 44 */ ... /* size: 840, cachelines: 14, members: 47 */ /* sum members: 801, holes: 8, sum holes: 35 */ /* padding: 4 */ /* paddings: 1, sum paddings: 4 */ /* last cacheline: 8 bytes */ }; As a result, the RSS key passed to the device is shifted by 1 byte: the last byte is cut off, and instead a (possibly uninitialized) byte is added at the beginning. As a last note `struct virtio_net_rss_config_hdr *rss_hdr;` is also moved to the end, since it seems those three members should stick around together. :)	N/A	More Details
CVE-2026-23142	In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs-scheme: cleanup access_pattern subdirs on scheme dir setup failure When a DAMOS-scheme DAMON sysfs directory setup fails after setup of access_pattern/ directory, subdirectories of access_pattern/ directory are not cleaned up. As a result, DAMON sysfs interface is nearly broken until the system reboots, and the memory for the unremoved directory is leaked. Cleanup the directories under such failures.	N/A	More Details
CVE-2026-23141	In the Linux kernel, the following vulnerability has been resolved: btrfs: send: check for inline extents in range_is_hole_in_parent() Before accessing the disk_bytenr field of a file extent item we need to check if we are dealing with an inline extent. This is because for inline extents their data starts at the offset of the disk_bytenr field. So accessing the disk_bytenr means we are accessing inline data or in case the inline data is less than 8 bytes we can actually cause an invalid memory access if this inline extent item is the first item in the leaf or access metadata from other items.	N/A	More Details
CVE-2026-23140	In the Linux kernel, the following vulnerability has been resolved: bpf, test_run: Subtract size of xdp_frame from allowed metadata size The xdp_frame structure takes up part of the XDP frame headroom, limiting the size of the metadata. However, in bpf_test_run, we don't take this into account, which makes it possible for userspace to supply a metadata size that is too large (taking up the entire headroom). If userspace supplies such a large metadata size in live packet mode, the xdp_update_frame_from_buff() call in xdp_test_run_init_page() call will fail, after which packet transmission proceeds with an uninitialised frame structure, leading to the usual Bad Stuff. The commit in the Fixes tag fixed a related bug where the second check in xdp_update_frame_from_buff() could fail, but did not add any additional constraints on the metadata size. Complete the fix by adding an additional check on the metadata size. Reorder the checks slightly to make the logic clearer and add a comment.	N/A	More Details
CVE-2026-23139	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conncount: update last_gc only when GC has been performed Currently last_gc is being updated everytime a new connection is tracked, that means that it is updated even if a GC wasn't performed. With a sufficiently high packet rate, it is possible to always bypass the GC, causing the list to grow infinitely. Update the last_gc value only when a GC has been actually performed.	N/A	More Details
CVE-2026-23138	In the Linux kernel, the following vulnerability has been resolved: tracing: Add recursion protection in kernel stack trace recording A bug was reported about an infinite recursion caused by tracing the rcu events with the kernel stack trace trigger enabled. The stack trace code called back into RCU which then called the stack trace again. Expand the ftrace recursion protection to add a set of bits to protect events from recursion. Each bit represents the context that the event is in (normal, softirq, interrupt and NMI). Have the stack trace code use the interrupt context to protect against recursion. Note, the bug showed an issue in both the RCU code as well as the tracing stacktrace code. This only handles the tracing stack trace side of the bug. The RCU fix will be handled separately.	N/A	More Details
CVE-2026-23137	In the Linux kernel, the following vulnerability has been resolved: of: unittest: Fix memory leak in unittest_data_add() In unittest_data_add(), if of_resolve_phandles() fails, the allocated unittest_data is not freed, leading to a memory leak. Fix this by using scope-based cleanup helper __free(kfree) for automatic resource cleanup. This ensures unittest_data is automatically freed when it goes out of scope in error paths. For the success path, use retain_and_null_ptr() to transfer ownership of the memory to the device tree and prevent double freeing.	N/A	More Details
CVE-2026-23136	In the Linux kernel, the following vulnerability has been resolved: libceph: reset sparse-read state in osd_fault() When a fault occurs, the connection is abandoned, reestablished, and any pending operations are retried. The OSD client tracks the progress of a sparse-read reply using a separate state machine, largely independent of the messenger's state. If a connection is lost mid-payload or the sparse-read state machine returns an error, the sparse-read state is not reset. The OSD client will then interpret the beginning of a new reply as the continuation of the old one. If this makes the sparse-read machinery enter a failure state, it may never recover, producing loops like: libceph: [0] got 0 extents libceph: data len 142248331 != extent len 0 libceph: osd0 (1)...:6801 socket error on read libceph: data len 142248331 != extent len 0 libceph: osd0 (1)...:6801 socket error on read Therefore, reset the sparse-read state in osd_fault(), ensuring retries start from a clean state.	N/A	More Details
CVE-2026-23135	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix dma_free_coherent() pointer dma_alloc_coherent() allocates a DMA mapped buffer and stores the addresses in XXX_unaligned fields. Those should be reused when freeing the buffer rather than the aligned addresses.	N/A	More Details
CVE-2026-23134	In the Linux kernel, the following vulnerability has been resolved: slab: fix kmalloc_nolock() context check for PREEMPT_RT On PREEMPT_RT kernels, local_lock becomes a sleeping lock. The current check in kmalloc_nolock() only verifies we're not in NMI or hard IRQ context, but misses the case where preemption is disabled. When a BPF program runs from a tracepoint with preemption disabled (preempt_count > 0), kmalloc_nolock() proceeds to call local_lock_irqsave() which attempts to acquire a sleeping lock, triggering: BUG: sleeping function called from invalid context in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 6128 preempt_count: 2, expected: 0 Fix this by checking !preemptible() on PREEMPT_RT, which directly expresses the constraint that we cannot take a sleeping lock when preemption is disabled. This encompasses the previous checks for NMI and hard IRQ contexts while also catching cases where preemption is disabled.	N/A	More Details
CVE-2026-23133	In the Linux kernel, the following vulnerability has been resolved: wifi: ath10k: fix dma_free_coherent() pointer dma_alloc_coherent() allocates a DMA mapped buffer and stores the addresses in XXX_unaligned fields. Those should be reused when freeing the buffer rather than the aligned addresses.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/bridge: synopsys: dw-dp: fix error paths of dw_dp_bind Fix several issues in dw_dp_bind() error handling: 1. Missing return after drm_bridge_attach() failure - the function continued		

CVE-2026-23132	execution instead of returning an error. 2. Resource leak: drm_dp_aux_register() is not a devm function, so drm_dp_aux_unregister() must be called on all error paths after aux registration succeeds. This affects errors from: - drm_bridge_attach() - phy_init() - devm_add_action_or_reset() - platform_get_irq() - devm_request_threaded_irq() 3. Bug fix: platform_get_irq() returns the IRQ number or a negative error code, but the error path was returning ERR_PTR(ret) instead of ERR_PTR(dp->irq). Use a goto label for cleanup to ensure consistent error handling.	N/A	More Details
CVE-2025-71202	In the Linux kernel, the following vulnerability has been resolved: iommu/sva: invalidate stale IOTLB entries for kernel address space Introduce a new IOMMU interface to flush IOTLB paging cache entries for the CPU kernel address space. This interface is invoked from the x86 architecture code that manages combined user and kernel page tables, specifically before any kernel page table page is freed and reused. This addresses the main issue with vfree() which is a common occurrence and can be triggered by unprivileged users. While this resolves the primary problem, it doesn't address some extremely rare case related to memory unplug of memory that was present as reserved memory at boot, which cannot be triggered by unprivileged users. The discussion can be found at the link below. Enable SVA on x86 architecture since the IOMMU can now receive notification to flush the paging cache before freeing the CPU kernel page table pages.	N/A	More Details
CVE-2025-71201	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix early read unlock of page with EOF in middle The read result collection for buffered reads seems to run ahead of the completion of subrequests under some circumstances, as can be seen in the following log snippet: 9p_client_res: client 18446612686390831168 response P9_TREAD tag 0 err 0 ... netfs_sreq: R=00001b55[1] DOWN TERM f=192 s=0 5fb2/5fb2 s=5 e=0 ... netfs_collect_folio: R=00001b55 ix=00004 r=4000-5000 t=4000/5fb2 netfs_folio: i=157f3 ix=00004-00004 read-done netfs_folio: i=157f3 ix=00004-00004 read-unlock netfs_collect_folio: R=00001b55 ix=00005 r=5000-5fb2 t=5000/5fb2 netfs_folio: i=157f3 ix=00005-00005 read-done netfs_folio: i=157f3 ix=00005-00005 read-unlock ... netfs_collect_stream: R=00001b55[0:] cto=5fb2 frn=ffffffff netfs_collect_state: R=00001b55 col=5fb2 cln=6000 n=c netfs_collect_stream: R=00001b55[0:] cto=5fb2 frn=ffffffff netfs_collect_state: R=00001b55 col=5fb2 cln=6000 n=8 ... netfs_sreq: R=00001b55[2] ZERO SUBMT f=000 s=5fb2 0/4e s=0 e=0 netfs_sreq: R=00001b55[2] ZERO TERM f=102 s=5fb2 4e/4e s=5 e=0 The 'cto=5fb2' indicates the collected file pos we've collected results to so far - but we still have 0x4e more bytes to go - so we shouldn't have collected folio ix=00005 yet. The 'ZERO' subreq that clears the tail happens after we unlock the folio, allowing the application to see the uncleared tail through mmap. The problem is that netfs_read_unlock_folios() will unlock a folio in which the amount of read results collected hits EOF position - but the ZERO subreq lies beyond that and so happens after. Fix this by changing the end check to always be the end of the folio and never the end of the file. In the future, I should look at clearing to the end of the folio here rather than adding a ZERO subreq to do this. On the other hand, the ZERO subreq can run in parallel with an async READ subreq. Further, the ZERO subreq may still be necessary to, say, handle extents in a ceph file that don't have any backing store and are thus implicitly all zeros. This can be reproduced by creating a file, the size of which doesn't align to a page boundary, e.g. 24998 (0x5fb2) bytes and then doing something like: xfs_io -c "mmap -r 0 0x6000" -c "madvise -d 0 0x6000" \ -c "mread -v 0 0x6000" /xfstest.test/x The last 0x4e bytes should all be 00, but if the tail hasn't been cleared yet, you may see rubbish there. This can be reproduced with kafs by modifying the kernel to disable the call to netfs_read_subreq_progress() and to stop afs_issue_read() from doing the async call for NETFS_READAHEAD. Reproduction can be made easier by inserting an mdelay(100) in netfs_issue_read() for the ZERO-subreq case. AFS and CIFS are normally unlikely to show this as they dispatch READ ops asynchronously, which allows the ZERO-subreq to finish first. 9P's READ op is completely synchronous, so the ZERO-subreq will always happen after. It isn't seen all the time, though, because the collection may be done in a worker thread.	N/A	More Details
CVE-2026-23131	In the Linux kernel, the following vulnerability has been resolved: platform/x86: hp-bioscfg: Fix kobject warnings for empty attribute names The hp-bioscfg driver attempts to register kobjects with empty names when the HP BIOS returns attributes with empty name strings. This causes multiple kernel warnings: kobject: (00000000135fb5e6): attempted to be registered with empty name! WARNING: CPU: 14 PID: 3336 at lib/kobject.c:219 kobject_add_internal+0x2eb/0x310 Add validation in hp_init_bios_buffer_attribute() to check if the attribute name is empty after parsing it from the WMI buffer. If empty, log a debug message and skip registration of that attribute, allowing the module to continue processing other valid attributes.	N/A	More Details
CVE-2026-23130	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix dead lock while flushing management frames Commit [1] converted the management transmission work item into a wiphy work. Since a wiphy work can only run under wiphy lock protection, a race condition happens in below scenario: 1. a management frame is queued for transmission. 2. ath12k_mac_op_flush() gets called to flush pending frames associated with the hardware (i.e, vif being NULL). Then in ath12k_mac_flush() the process waits for the transmission done. 3. Since wiphy lock has been taken by the flush process, the transmission work item has no chance to run, hence the dead lock. >From user view, this dead lock results in below issue: wlp8s0: authenticate with xxxxxx (local address=xxxxxx) wlp8s0: send auth to xxxxxx (try 1/3) wlp8s0: authenticate with xxxxxx (local address=xxxxxx) wlp8s0: send auth to xxxxxx (try 1/3) wlp8s0: authenticated wlp8s0: associate with xxxxxx (try 1/3) wlp8s0: aborting association with xxxxxx by local choice (Reason: 3=DEAUTH_LEAVING) ath12k_pci 0000:08:00.0: failed to flush mgmt transmit queue, mgmt pkts pending 1 The dead lock can be avoided by invoking wiphy_work_flush() to proactively run the queued work item. Note actually it is already present in ath12k_mac_op_flush(), however it does not protect the case where vif being NULL. Hence move it ahead to cover this case as well. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1.c5-00302-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1.115823.3	N/A	More Details
CVE-2026-23129	In the Linux kernel, the following vulnerability has been resolved: dpll: Prevent duplicate registrations Modify the internal registration helpers dpll_xa_ref_{dpll,pin}_add() to reject duplicate registration attempts. Previously, if a caller attempted to register the same pin multiple times (with the same ops, priv, and cookie) on the same device, the core silently increments the reference count and return success. This behavior is incorrect because if the caller makes these duplicate registrations then for the first one dpll_pin_registration is allocated and for others the associated dpll_pin_ref.refcount is incremented. During the first unregistration the associated dpll_pin_registration is freed and for others WARN is fired. Fix this by updating the logic to return `-EEXIST` if a matching registration is found to enforce a strict "register once" policy.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: arm64: Set __nocfi on swsusp_arch_resume() A DABT is reported[1] on an android based system when resume from hiberate. This happens because swsusp_arch_suspend_exit() is marked with SYM_CODE_*() and does not have a CFI hash, but swsusp_arch_resume() will attempt to verify the CFI hash when calling a copy of swsusp_arch_suspend_exit(). Given that there's an existing requirement that the entrypoint to swsusp_arch_suspend_exit() is the first byte of the .hibernate_exit.text section, we cannot fix this by marking swsusp_arch_suspend_exit() with SYM_FUNC_*(). The simplest fix for now is to disable the CFI check in swsusp_arch_resume(). Mark swsusp_arch_resume() as __nocfi to disable the CFI check. [1] [22.991934][T1] Unable to handle kernel paging request at virtual address 0000000109170ffc [22.991934][T1] Mem abort info: [22.991934][T1] ESR = 0x0000000096000007 [22.991934][T1] EC = 0x25: DABT (current EL), IL = 32 bits [22.991934][T1] SET = 0, FnV = 0 [22.991934][T1] EA = 0,		

CVE-2026-23128	S1PTW = 0 [22.991934][T1] FSC = 0x07: level 3 translation fault [22.991934][T1] Data abort info: [22.991934][T1] ISV = 0, ISS = 0x00000007, ISS2 = 0x00000000 [22.991934][T1] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [22.991934][T1] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [22.991934][T1] [0000000109170ffc] user address but active_mm is swapper [22.991934][T1] Internal error: Oops: 0000000096000007 [#1] PREEMPT SMP [22.991934][T1] Dumping ftrace buffer: [22.991934][T1] (ftrace buffer empty) [22.991934][T1] Modules linked in: [22.991934][T1] CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.6.98-android15-8-g0b1d2aee7fc3-dirty-4k #1 688c7060a825a3ac418fe53881730b355915a419 [22.991934][T1] Hardware name: Unisoc UMS9360-base Board (DT) [22.991934][T1] pstate: 804000c5 (Nzcv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [22.991934][T1] pc : swsusp_arch_resume+0x2ac/0x344 [22.991934][T1] lr : swsusp_arch_resume+0x294/0x344 [22.991934][T1] sp : ffffffc08006b960 [22.991934][T1] x29: ffffffc08006b9c0 x28: 0000000000000000 x27: 0000000000000000 [22.991934][T1] x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000820 [22.991934][T1] x23: fffffffd0817e3000 x22: fffffffd0817e3000 x21: 0000000000000000 [22.991934][T1] x20: ffffff8089171000 x19: fffffffd08252c8c8 x18: ffffffc080061058 [22.991934][T1] x17: 00000000529c6ef0 x16: 00000000529c6ef0 x15: 0000000000000004 [22.991934][T1] x14: ffffff8178c88000 x13: 0000000000000006 x12: 0000000000000000 [22.991934][T1] x11: 0000000000000015 x10: 0000000000000001 x9 : fffffffd082533000 [22.991934][T1] x8 : 0000000109171000 x7 : 205b5d3433393139 x6 : 392e32322020205b [22.991934][T1] x5 : 000000010916f000 x4 : 000000008164b000 x3 : ffffff808a4e0530 [22.991934][T1] x2 : fffffffd08058e784 x1 : 0000000082326000 x0 : 000000010a283000 [22.991934][T1] Call trace: [22.991934][T1] swsusp_arch_resume+0x2ac/0x344 [22.991934][T1] hibernation_restore+0x158/0x18c [22.991934][T1] load_image_and_restore+0xb0/0xec [22.991934][T1] software_resume+0xf4/0x19c [22.991934][T1] software_resume_initcall+0x34/0x78 [22.991934][T1] do_one_initcall+0xe8/0x370 [22.991934][T1] do_initcall_level+0xc8/0x19c [22.991934][T1] do_initcalls+0x70/0xc0 [22.991934][T1] do_basic_setup+0x1c/0x28 [22.991934][T1] kernel_init_freeable+0xe0/0x148 [22.991934][T1] kernel_init+0x20/0x1a8 [22.991934][T1] ret_from_fork+0x10/0x20 [22.991934][T1] Code: a9400a61 f94013e0 f9438923 f9400a64 (b85fc110) [catalin.marinas@arm.com: commit log updated by Mark Rutland]	N/A	More Details
CVE-2026-23127	In the Linux kernel, the following vulnerability has been resolved: perf: Fix refcount warning on event->mmap_count increment When calling refcount_inc(&event->mmap_count) inside perf_mmap_rb(), the following warning is triggered: refcount_t: addition on 0; use-after-free. WARNING: lib/refcount.c:25 PoC: struct perf_event_attr attr = {0}; int fd = syscall(__NR_perf_event_open, &attr, 0, -1, -1, 0); mmap(NULL, 0x3000, PROT_READ | PROT_WRITE, MAP_SHARED, fd, 0); int victim = syscall(__NR_perf_event_open, &attr, 0, -1, fd, PERF_FLAG_FD_OUTPUT); mmap(NULL, 0x3000, PROT_READ | PROT_WRITE, MAP_SHARED, victim, 0); This occurs when creating a group member event with the flag PERF_FLAG_FD_OUTPUT. The group leader should be mmap-ed and then mmap-ing the event triggers the warning. Since the event has copied the output_event in perf_event_set_output(), event->rb is set. As a result, perf_mmap_rb() calls refcount_inc(&event->mmap_count) when event->mmap_count = 0. Disallow the case when event->mmap_count = 0. This also prevents two events from updating the same user_page.	N/A	More Details
CVE-2026-23126	In the Linux kernel, the following vulnerability has been resolved: netdevsim: fix a race issue related to the operation on bpf_bound_progs list The netdevsim driver lacks a protection mechanism for operations on the bpf_bound_progs list. When the nsim_bpf_create_prog() performs list_add_tail, it is possible that nsim_bpf_destroy_prog() is simultaneously performs list_del. Concurrent operations on the list may lead to list corruption and trigger a kernel crash as follows: [417.290971] kernel BUG at lib/list_debug.c:62! [417.290983] invalid opcode: 0000 [#1] PREEMPT SMP NOPTI [417.290992] CPU: 10 PID: 168 Comm: kworker/10:1 Kdump: loaded Not tainted 6.19.0-rc5 #1 [417.291003] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [417.291007] Workqueue: events bpf_prog_free_deferred [417.291021] RIP: 0010:__list_del_entry_valid_or_report+0xa7/0xc0 [417.291034] Code: a8 ff 0f 0b 48 89 fe 48 89 ca 48 c7 c7 48 a1 eb ae e8 ed fb a8 ff 0f 0b 48 89 fe 48 89 c2 48 c7 c7 80 a1 eb ae e8 d9 fb a8 ff <0f> 0b 48 89 d1 48 c7 c7 d0 a1 eb ae 48 89 f2 48 89 c6 e8 c2 fb a8 [417.291040] RSP: 0018:ffffb16a40807df8 EFLAGS: 00010246 [417.291046] RAX: 000000000000006d RBX: ffff8e589866f500 RCX: 0000000000000000 [417.291051] RDX: 0000000000000000 RSI: ffff8e59f7b23180 RDI: ffff8e59f7b23180 [417.291055] RBP: ffffb16a412c9000 R08: 0000000000000000 R09: 0000000000000003 [417.291059] R10: ffffb16a40807c80 R11: ffffffffaf9edce8 R12: ffff8e594427ac20 [417.291063] R13: ffff8e59f7b44780 R14: ffff8e58800b7a05 R15: 0000000000000000 [417.291074] FS: 0000000000000000(0000) GS:ffff8e59f7b00000(0000) knlGS:0000000000000000 [417.291079] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [417.291083] CR2: 00007fc4083efe08 CR3: 00000001c3626006 CR4: 0000000000770ee0 [417.291088] PKRU: 55555554 [417.291091] Call Trace: [417.291096] <TASK> [417.291103] nsim_bpf_destroy_prog+0x31/0x80 [netdevsim] [417.291154] __bpf_prog_offload_destroy+0x2a/0x80 [417.291163] bpf_prog_dev_bound_destroy+0x6f/0xb0 [417.291171] bpf_prog_free_deferred+0x18e/0x1a0 [417.291178] process_one_work+0x18a/0x3a0 [417.291188] worker_thread+0x27b/0x3a0 [417.291197] ? __pfx_worker_thread+0x10/0x10 [417.291207] kthread+0xe5/0x120 [417.291214] ? __pfx_kthread+0x10/0x10 [417.291221] ret_from_fork+0x31/0x50 [417.291230] ? __pfx_kthread+0x10/0x10 [417.291236] ret_from_fork_asm+0x1a/0x30 [417.291246] </TASK> Add a mutex lock, to prevent simultaneous addition and deletion operations on the list.	N/A	More Details
CVE-2026-23125	In the Linux kernel, the following vulnerability has been resolved: sctp: move SCTP_CMD_ASSOC_SHKEY right after SCTP_CMD_PEER_INIT A null-ptr-deref was reported in the SCTP transmit path when SCTP-AUTH key initialization fails: == KASAN: null-ptr-deref in range [0x0000000000000018-0x000000000000001f] CPU: 0 PID: 16 Comm: ksoftirqd/0 Tainted: G W 6.6.0 #2 RIP: 0010:sctp_packet_bundle_auth net/sctp/output.c:264 [inline] RIP: 0010:sctp_packet_append_chunk+0xb36/0x1260 net/sctp/output.c:401 Call Trace: sctp_packet_transmit_chunk+0x31/0x250 net/sctp/output.c:189 sctp_outq_flush_data+0xa29/0x26d0 net/sctp/outqueue.c:1111 sctp_outq_flush+0xc80/0x1240 net/sctp/outqueue.c:1217 sctp_cmd_interpreter.isra.0+0x19a5/0x62c0 net/sctp/sm_sideeffect.c:1787 sctp_side_effects net/sctp/sm_sideeffect.c:1198 [inline] sctp_do_sm+0x1a3/0x670 net/sctp/sm_sideeffect.c:1169 sctp_assoc_bh_rcv+0x33e/0x640 net/sctp/associola.c:1052 sctp_inq_push+0x1dd/0x280 net/sctp/inqueue.c:88 sctp_rcv+0x11ae/0x3100 net/sctp/input.c:243 sctp6_rcv+0x3d/0x60 net/sctp/ipv6.c:1127 The issue is triggered when sctp_auth_asoc_init_active_key() fails in sctp_sf_do_5_1C_ack() while processing an INIT_ACK. In this case, the command sequence is currently: - SCTP_CMD_PEER_INIT - SCTP_CMD_TIMER_STOP (T1_INIT) - SCTP_CMD_TIMER_START (T1_COOKIE) - SCTP_CMD_NEW_STATE (COOKIE_ECHOED) - SCTP_CMD_ASSOC_SHKEY - SCTP_CMD_GEN_COOKIE_ECHO If SCTP_CMD_ASSOC_SHKEY fails, asoc->shkey remains NULL, while asoc->peer.auth_capable and asoc->peer.peer_chunks have already been set by SCTP_CMD_PEER_INIT. This allows a DATA chunk with auth = 1 and shkey = NULL to be queued by sctp_datamsg_from_user(). Since command interpretation stops on failure, no COOKIE_ECHO should been sent via SCTP_CMD_GEN_COOKIE_ECHO. However, the T1_COOKIE timer has already been started, and it may enqueue a COOKIE_ECHO into the outqueue later. As a result, the DATA chunk can be transmitted together with the COOKIE_ECHO in sctp_outq_flush_data(), leading to the observed issue. Similar to the other places where it calls sctp_auth_asoc_init_active_key() right after sctp_process_init(), this patch moves the SCTP_CMD_ASSOC_SHKEY immediately after SCTP_CMD_PEER_INIT, before stopping T1_INIT and starting T1_COOKIE. This ensures that if shared key generation fails,	N/A	More Details

	authenticated DATA cannot be sent. It also allows the T1_INIT timer to retransmit INIT, giving the client another chance to process INIT_ACK and retry key setup.		
CVE-2026-23124	In the Linux kernel, the following vulnerability has been resolved: ipv6: annotate data-race in ndisc_router_discovery() syzbot found that ndisc_router_discovery() could read and write in6_dev->ra_mtu without holding a lock [1] This looks fine, IFLA_INET6_RA_MTU is best effort. Add READ_ONCE()/WRITE_ONCE() to document the race. Note that we might also reject illegal MTU values (mtu < IPV6_MIN_MTU || mtu > skb->dev->mtu) in a future patch. [1] BUG: KCSAN: data-race in ndisc_router_discovery / ndisc_router_discovery read to 0xffff888119809c20 of 4 bytes by task 25817 on cpu 1: ndisc_router_discovery+0x151d/0x1c90 net/ipv6/ndisc.c:1558 ndisc_rcv+0x2ad/0x3d0 net/ipv6/ndisc.c:1841 icmpv6_rcv+0xe5a/0x12f0 net/ipv6/icmp.c:989 ip6_protocol_deliver_rcu+0xb2a/0x10d0 net/ipv6/ip6_input.c:438 ip6_input_finish+0xf0/0x1d0 net/ipv6/ip6_input.c:489 NF_HOOK include/linux/netfilter.h:318 [inline] ip6_input+0x5e/0x140 net/ipv6/ip6_input.c:500 ip6_mc_input+0x27c/0x470 net/ipv6/ip6_input.c:590 dst_input include/net/dst.h:474 [inline] ip6_rcv_finish+0x336/0x340 net/ipv6/ip6_input.c:79 ... write to 0xffff888119809c20 of 4 bytes by task 25816 on cpu 0: ndisc_router_discovery+0x155a/0x1c90 net/ipv6/ndisc.c:1559 ndisc_rcv+0x2ad/0x3d0 net/ipv6/ndisc.c:1841 icmpv6_rcv+0xe5a/0x12f0 net/ipv6/icmp.c:989 ip6_protocol_deliver_rcu+0xb2a/0x10d0 net/ipv6/ip6_input.c:438 ip6_input_finish+0xf0/0x1d0 net/ipv6/ip6_input.c:489 NF_HOOK include/linux/netfilter.h:318 [inline] ip6_input+0x5e/0x140 net/ipv6/ip6_input.c:500 ip6_mc_input+0x27c/0x470 net/ipv6/ip6_input.c:590 dst_input include/net/dst.h:474 [inline] ip6_rcv_finish+0x336/0x340 net/ipv6/ip6_input.c:79 ... value changed: 0x00000000 -> 0xe5400659	N/A	More Details
CVE-2026-23123	In the Linux kernel, the following vulnerability has been resolved: interconnect: debugfs: initialize src_node and dst_node to empty strings The debugfs_create_str() API assumes that the string pointer is either NULL or points to valid kmalloc() memory. Leaving the pointer uninitialized can cause problems. Initialize src_node and dst_node to empty strings before creating the debugfs entries to guarantee that reads and writes are safe.	N/A	More Details
CVE-2026-23122	In the Linux kernel, the following vulnerability has been resolved: igc: Reduce TSN TX packet buffer from 7KB to 5KB per queue The previous 7 KB per queue caused TX unit hangs under heavy timestamping load. Reducing to 5 KB avoids these hangs and matches the TSN recommendation in I225/I226 SW User Manual Section 7.5.4. The 8 KB "freed" by this change is currently unused. This reduction is not expected to impact throughput, as the i226 is PCIe-limited for small TSN packets rather than TX-buffer-limited.	N/A	More Details
CVE-2026-23121	In the Linux kernel, the following vulnerability has been resolved: mISDN: annotate data-race around dev->work dev->work can re read locklessly in mISDN_read() and mISDN_poll(). Add READ_ONCE()/WRITE_ONCE() annotations. BUG: KCSAN: data-race in mISDN_ioctl / mISDN_read write to 0xffff88812d848280 of 4 bytes by task 10864 on cpu 1: misdn_add_timer drivers/isdn/mISDN/timerdev.c:175 [inline] mISDN_ioctl+0x2fb/0x550 drivers/isdn/mISDN/timerdev.c:233 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl+0xce/0x140 fs/ioctl.c:583 __x64_sys_ioctl+0x43/0x50 fs/ioctl.c:583 x64_sys_call+0x14b0/0x3000 arch/x86/include/generated/asm/syscalls_64.h:17 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xd8/0x2c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f read to 0xffff88812d848280 of 4 bytes by task 10857 on cpu 0: mISDN_read+0x1f2/0x470 drivers/isdn/mISDN/timerdev.c:112 do_loop_readv_writev fs/read_write.c:847 [inline] vfs_readv+0x3fb/0x690 fs/read_write.c:1020 do_readv+0xe7/0x210 fs/read_write.c:1080 __do_sys_readv fs/read_write.c:1165 [inline] __se_sys_readv fs/read_write.c:1162 [inline] __x64_sys_readv+0x45/0x50 fs/read_write.c:1162 x64_sys_call+0x2831/0x3000 arch/x86/include/generated/asm/syscalls_64.h:20 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xd8/0x2c0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f value changed: 0x00000000 -> 0x00000001	N/A	More Details
CVE-2026-23120	In the Linux kernel, the following vulnerability has been resolved: l2tp: avoid one data-race in l2tp_tunnel_del_work() We should read sk->sk_socket only when dealing with kernel sockets. syzbot reported the following data-race: BUG: KCSAN: data-race in l2tp_tunnel_del_work / sk_common_release write to 0xffff88811c182b20 of 8 bytes by task 5365 on cpu 0: sk_set_socket include/net/sock.h:2092 [inline] sock_orphan include/net/sock.h:2118 [inline] sk_common_release+0xae/0x230 net/core/sock.c:4003 udp_lib_close+0x15/0x20 include/net/udp.h:325 inet_release+0xce/0xf0 net/ipv4/af_inet.c:437 __sock_release net/socket.c:662 [inline] sock_close+0x6b/0x150 net/socket.c:1455 __fput+0x29b/0x650 fs/file_table.c:468 ____fput+0x1c/0x30 fs/file_table.c:496 task_work_run+0x131/0x1a0 kernel/task_work.c:233 resume_user_mode_work include/linux/resume_user_mode.h:50 [inline] __exit_to_user_mode_loop kernel/entry/common.c:44 [inline] exit_to_user_mode_loop+0x1fe/0x740 kernel/entry/common.c:75 __exit_to_user_mode_prepare include/linux/irq-entry-common.h:226 [inline] syscall_exit_to_user_mode_prepare include/linux/irq-entry-common.h:256 [inline] syscall_exit_to_user_mode_work include/linux/entry-common.h:159 [inline] syscall_exit_to_user_mode include/linux/entry-common.h:194 [inline] do_syscall_64+0x1e1/0x2b0 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f read to 0xffff88811c182b20 of 8 bytes by task 827 on cpu 1: l2tp_tunnel_del_work+0x2f/0x1a0 net/l2tp/l2tp_core.c:1418 process_one_work kernel/workqueue.c:3257 [inline] process_scheduled_works+0x4ce/0x9d0 kernel/workqueue.c:3340 worker_thread+0x582/0x770 kernel/workqueue.c:3421 kthread+0x489/0x510 kernel/kthread.c:463 ret_from_fork+0x149/0x290 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:246 value changed: 0xffff88811b818000 -> 0x0000000000000000	N/A	More Details
CVE-2026-23145	In the Linux kernel, the following vulnerability has been resolved: ext4: fix iloc.bh leak in ext4_xattr_inode_update_ref The error branch for ext4_xattr_inode_update_ref forget to release the refcount for iloc.bh. Find this when review code.	N/A	More Details
CVE-2026-23146	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_uart: fix null-ptr-deref in hci_uart_write_work hci_uart_set_proto() sets HCI_UART_PROTO_INIT before calling hci_uart_register_dev(), which calls proto->open() to initialize hu->priv. However, if a TTY write wakeup occurs during this window, hci_uart_tx_wakeup() may schedule write_work before hu->priv is initialized, leading to a NULL pointer dereference in hci_uart_write_work() when proto->dequeue() accesses hu->priv. The race condition is: CPU0 CPU1 ---- ---- hci_uart_set_proto() set_bit(HCI_UART_PROTO_INIT) hci_uart_register_dev() tty write wakeup hci_uart_tty_wakeup() hci_uart_tx_wakeup() schedule_work(&hu->write_work) proto->open(hu) // initializes hu->priv hci_uart_write_work() hci_uart_dequeue() proto->dequeue(hu) // accesses hu->priv (NULL!) Fix this by moving set_bit(HCI_UART_PROTO_INIT) after proto->open() succeeds, ensuring hu->priv is initialized before any work can be scheduled.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: btrfs: zlib: fix the folio leak on S390 hardware acceleration [BUG] After commit aa60fe12b4f4 ("btrfs: zlib: refactor S390x HW acceleration buffer preparation"), we no longer release the folio of the page cache of folio returned by btrfs_compress_filemap_get_folio() for S390 hardware acceleration path. [CAUSE] Before that commit, we call kumap_local() and folio_put() after handling each folio. Although the timing is not ideal (it release	N/A	More

23147	previous folio at the beginning of the loop, and rely on some extra cleanup out of the loop), it at least handles the folio release correctly. Meanwhile the refactored code is easier to read, it lacks the call to release the filemap folio. [FIX] Add the missing folio_put() for copy_data_into_buffer().		Details
CVE-2026-23162	In the Linux kernel, the following vulnerability has been resolved: drm/xe/nvm: Fix double-free on aux add failure After a successful auxiliary_device_init(), aux_dev->dev.release (xe_nvm_release_dev()) is responsible for the kfree(nvm). When there is failure with auxiliary_device_add(), driver will call auxiliary_device_uninit(), which call put_device(). So that the .release callback will be triggered to free the memory associated with the auxiliary_device. Move the kfree(nvm) into the auxiliary_device_init() failure path and remove the err goto path to fix below error. " [13.232905] == [13.232911] BUG: KASAN: double-free in xe_nvm_init+0x751/0xf10 [xe] [13.233112] Free of addr ffff888120635000 by task systemd-udevd/273 [13.233120] CPU: 8 UID: 0 PID: 273 Comm: systemd-udevd Not tainted 6.19.0-rc2-lgci-xe-kernel+ #225 PREEMPT(voluntary) ... [13.233125] Call Trace: [13.233126] <TASK> [13.233127] dump_stack_lvl+0x7f/0xc0 [13.233132] print_report+0xce/0x610 [13.233136] ? kasan_complete_mode_report_info+0x5d/0x1e0 [13.233139] ? xe_nvm_init+0x751/0xf10 [xe] ... " v2: drop err goto path. (Alexander) (cherry picked from commit a3187c0c2bbd947ffff97f90d077ac88f9c2a215)	N/A	More Details
CVE-2025-71203	In the Linux kernel, the following vulnerability has been resolved: riscv: Sanitize syscall table indexing under speculation The syscall number is a user-controlled value used to index into the syscall table. Use array_index_nospec() to clamp this value after the bounds check to prevent speculative out-of-bounds access and subsequent data leakage via cache side channels.	N/A	More Details
CVE-2026-23173	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: TC, delete flows only for existing peers When deleting TC steering flows, iterate only over actual devcom peers instead of assuming all possible ports exist. This avoids touching non-existent peers and ensures cleanup is limited to devices the driver is currently connected to. BUG: kernel NULL pointer dereference, address: 0000000000000008 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 133c8a067 P4D 0 Oops: Oops: 0002 [#1] SMP CPU: 19 UID: 0 PID: 2169 Comm: tc Not tainted 6.18.0+ #156 NONE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:mlx5e_tc_del_fdb_peers_flow+0xbe/0x200 [mlx5_core] Code: 00 00 a8 08 74 a8 49 8b 46 18 f6 c4 02 74 9f 4c 8d bf a0 12 00 00 4c 89 ff e8 0e e7 96 e1 49 8b 44 24 08 49 8b 0c 24 4c 89 ff <48> 89 41 08 48 89 08 49 89 2c 24 49 89 5c 24 08 e8 7d ce 96 e1 49 RSP: 0018:ff11000143867528 EFLAGS: 00010246 RAX: 0000000000000000 RBX: dead000000000122 RCX: 0000000000000000 RDX: ff11000143691580 RSI: ff110001026e5000 RDI: ff11000106f3d2a0 RBP: dead000000000100 R08: 00000000000003fd R09: 0000000000000002 R10: ff11000101c75690 R11: ff1100085faea178 R12: ff11000115f0ae78 R13: 0000000000000000 R14: ff11000115f0a800 R15: ff11000106f3d2a0 FS: 00007f35236bf740(0000) GS:ff110008dc809000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 0000000157a01001 CR4: 0000000000373eb0 Call Trace: <TASK> mlx5e_tc_del_flow+0x46/0x270 [mlx5_core] mlx5e_flow_put+0x25/0x50 [mlx5_core] mlx5e_delete_flower+0x2a6/0x3e0 [mlx5_core] tc_setup_cb_reoffload+0x20/0x80 fl_reoffload+0x26f/0x2f0 [cls_flower] ? mlx5e_tc_reoffload_flows_work+0xc0/0xc0 [mlx5_core] ? mlx5e_tc_reoffload_flows_work+0xc0/0xc0 [mlx5_core] tcf_block_playback_offloads+0x9e/0x1c0 tcf_block_unbind+0x7b/0xd0 tcf_block_setup+0x186/0x1d0 tcf_block_offload_cmd.isra.0+0xef/0x130 tcf_block_offload_unbind+0x43/0x70 __tcf_block_put+0x85/0x160 ingress_destroy+0x32/0x110 [sch_ingress] __qdisc_destroy+0x44/0x100 qdisc_graft+0x22b/0x610 tc_get_qdisc+0x183/0x4d0 rtnetlink_rcv_msg+0x2d7/0x3d0 ? rtnl_calcit.isra.0+0x100/0x100 netlink_rcv_skb+0x53/0x100 netlink_unicast+0x249/0x320 ? __alloc_skb+0x102/0x1f0 netlink_sendmsg+0x1e3/0x420 __sock_sendmsg+0x38/0x60 ____sys_sendmsg+0x1ef/0x230 ? copy_msghdr_from_user+0x6c/0xa0 ___sys_sendmsg+0x7f/0xc0 ? ___sys_recvmsg+0x8a/0xc0 ? __sys_sendto+0x119/0x180 __sys_sendmsg+0x61/0xb0 do_syscall_64+0x55/0x640 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f35238bb764 Code: 15 b9 86 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bf 0f 1f 44 00 00 f3 0f 1e fa 80 3d e5 08 0d 00 00 74 13 b8 2e 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 4c c3 0f 1f 00 55 48 89 e5 48 83 ec 20 89 55 RSP: 002b:00007ffed4c35638 EFLAGS: 00000202 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 000055a2efcc75e0 RCX: 00007f35238bb764 RDX: 0000000000000000 RSI: 00007ffed4c356a0 RDI: 0000000000000003 RBP: 00007ffed4c35710 R08: 0000000000000010 R09: 00007f3523984b20 R10: 0000000000000004 R11: 0000000000000202 R12: 00007ffed4c35790 R13: 000000006947df8f R14: 000055a2efcc75e0 R15: 00007ffed4c35780	N/A	More Details
CVE-2026-23172	In the Linux kernel, the following vulnerability has been resolved: net: wwan: t7xx: fix potential skb->frags overflow in RX path When receiving data in the DPMAIF RX path, the t7xx_dpmaif_set_frag_to_skb() function adds page fragments to an skb without checking if the number of fragments has exceeded MAX_SKB_FRAGS. This could lead to a buffer overflow in skb_shinfo(skb)->frags[] array, corrupting adjacent memory and potentially causing kernel crashes or other undefined behavior. This issue was identified through static code analysis by comparing with a similar vulnerability fixed in the mt76 driver commit b102f0c522cf ("mt76: fix array overflow on receiving too many fragments for a packet"). The vulnerability could be triggered if the modem firmware sends packets with excessive fragments. While under normal protocol conditions (MTU 3080 bytes, BAT buffer 3584 bytes), a single packet should not require additional fragments, the kernel should not blindly trust firmware behavior. Malicious, buggy, or compromised firmware could potentially craft packets with more fragments than the kernel expects. Fix this by adding a bounds check before calling skb_add_rx_frag() to ensure nr_frags does not exceed MAX_SKB_FRAGS. The check must be performed before unmapping to avoid a page leak and double DMA unmap during device teardown.	N/A	More Details
CVE-2026-23171	In the Linux kernel, the following vulnerability has been resolved: bonding: fix use-after-free due to enslave fail after slave array update Fix a use-after-free which happens due to enslave failure after the new slave has been added to the array. Since the new slave can be used for Tx immediately, we can use it after it has been freed by the enslave error cleanup path which frees the allocated slave memory. Slave update array is supposed to be called last when further enslave failures are not expected. Move it after xdp setup to avoid any problems. It is very easy to reproduce the problem with a simple xdp_pass prog: ip l add bond1 type bond mode balance-xor ip l set bond1 up ip l set dev bond1 xdp object xdp_pass.o sec xdp_pass ip l add dumdum type dummy Then run in parallel: while :; do ip l set dumdum master bond1 1>/dev/null 2>&1; done; mausezahn bond1 -a own -b rand -A rand -B 1.1.1.1 -c 0 -t tcp "dp=1-1023, flags=syn" The crash happens almost immediately: [605.602850] Oops: general protection fault, probably for non-canonical address 0xe0e6fc2460000137: 0000 [#1] SMP KASAN NOPTI [605.602916] KASAN: maybe wild-memory-access in range [0x07380123000009b8-0x07380123000009bf] [605.602946] CPU: 0 UID: 0 PID: 2445 Comm: mausezahn Kdump: loaded Tainted: G B 6.19.0-rc6+ #21 PREEMPT(voluntary) [605.602979] Tainted: [B]=BAD_PAGE [605.602998] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [605.603032] RIP: 0010:netdev_core_pick_tx+0xcd/0x210 [605.603063] Code: 48 89 fa 48 c1 ea 03 80 3c 02 00 0f 85 3e 01 00 00 48 b8 00 00 00 00 00 fc ff df 4c 8b 6b 08 49 8d 7d 30 48 89 fa 48 c1 ea 03 <80> 3c 02 00 0f 85 25 01 00 00 49 8b 45 30 4c 89 e2 48 89 ee 48 89 [605.603111] RSP: 0018:ffff88817b9af348 EFLAGS: 00010213 [605.603145] RAX:	N/A	More Details

	dfffc0000000000 RBX: ffff88817d28b420 RCX: 0000000000000000 [605.603172] RDX: 00e7002460000137 RSI: 0000000000000008 RDI: 07380123000009be [605.603199] RBP: ffff88817b541a00 R08: 0000000000000001 R09: fffffbfff3ed8c0c [605.603226] R10: ffffffff9f6c6067 R11: 0000000000000001 R12: 0000000000000000 [605.603253] R13: 073801230000098e R14: ffff88817d28b448 R15: ffff88817b541a84 [605.603286] FS: 00007f6570ef67c0(0000) GS:ffff888221dfa000(0000) knlGS:0000000000000000 [605.603319] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [605.603343] CR2: 00007f65712fae40 CR3: 000000011371b000 CR4: 0000000000350ef0 [605.603373] Call Trace: [605.603392] <TASK> [605.603410] __dev_queue_xmit+0x448/0x32a0 [605.603434] ? __pfx_vprintk_emit+0x10/0x10 [605.603461] ? __pfx_vprintk_emit+0x10/0x10 [605.603484] ? __pfx___dev_queue_xmit+0x10/0x10 [605.603507] ? bond_start_xmit+0xbfb/0xc20 [bonding] [605.603546] ? _printk+0xcb/0x100 [605.603566] ? __pfx__printk+0x10/0x10 [605.603589] ? bond_start_xmit+0xbfb/0xc20 [bonding] [605.603627] ? add_taint+0x5e/0x70 [605.603648] ? add_taint+0x2a/0x70 [605.603670] ? end_report.cold+0x51/0x75 [605.603693] ? bond_start_xmit+0xbfb/0xc20 [bonding] [605.603731] bond_start_xmit+0x623/0xc20 [bonding]		
CVE-2026-23170	In the Linux kernel, the following vulnerability has been resolved: drm/imx/tve: fix probe device leak Make sure to drop the reference taken to the DDC device during probe on probe failure (e.g. probe deferral) and on driver unbind.	N/A	More Details
CVE-2026-23169	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix race in mptcp_pm_nl_flush_addrs_doit() syzbot and Eulgyu Kim reported crashes in mptcp_pm_nl_get_local_id() and/or mptcp_pm_nl_is_backup() Root cause is list_splice_init() in mptcp_pm_nl_flush_addrs_doit() which is not RCU ready. list_splice_init_rcu() can not be called here while holding pernet->lock spinlock. Many thanks to Eulgyu Kim for providing a repro and testing our patches.	N/A	More Details
CVE-2026-23168	In the Linux kernel, the following vulnerability has been resolved: flex_proportions: make fprop_new_period() hardirq safe Bernd has reported a lockdep splat from flexible proportions code that is essentially complaining about the following race: <timer fires> run_timer_softirq - we are in softirq context call_timer_fn writeout_period fprop_new_period write_seqcount_begin(&p->sequence); <hardirq is raised> ... blk_mq_end_request() blk_update_request() ext4_end_bio() folio_end_writeback() __wb_writeout_add() __fprop_add_percpu_max() if (unlikely(max_frac < FPROP_FRAC_BASE)) { fprop_fraction_percpu() seq = read_seqcount_begin(&p->sequence); - sees odd sequence so loops indefinitely Note that a deadlock like this is only possible if the bdi has configured maximum fraction of writeout throughput which is very rare in general but frequent for example for FUSE bdis. To fix this problem we have to make sure write section of the sequence counter is irqsafe.	N/A	More Details
CVE-2026-23167	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: Fix race between rfkill and nci_unregister_device(). syzbot reported the splat below [0] without a repro. It indicates that struct nci_dev.cmd_wq had been destroyed before nci_close_device() was called via rfkill. nci_dev.cmd_wq is only destroyed in nci_unregister_device(), which (I think) was called from virtual_ncidev_close() when syzbot close()d an fd of virtual_ncidev. The problem is that nci_unregister_device() destroys nci_dev.cmd_wq first and then calls nfc_unregister_device(), which removes the device from rfkill by rfkill_unregister(). So, the device is still visible via rfkill even after nci_dev.cmd_wq is destroyed. Let's unregister the device from rfkill first in nci_unregister_device(). Note that we cannot call nfc_unregister_device() before nci_close_device() because 1) nfc_unregister_device() calls device_del() which frees all memory allocated by devm_kzalloc() and linked to ndev->conn_info_list 2) nci_rx_work() could try to queue nci_conn_info to ndev->conn_info_list which could be leaked Thus, nfc_unregister_device() is split into two functions so we can remove rfkill interfaces only before nci_close_device(). [0]: DEBUG_LOCKS_WARN_ON(1) WARNING: kernel/locking/lockdep.c:238 at hlock_class kernel/locking/lockdep.c:238 [inline], CPU#0: syz.0.8675/6349 WARNING: kernel/locking/lockdep.c:238 at check_wait_context kernel/locking/lockdep.c:4854 [inline], CPU#0: syz.0.8675/6349 WARNING: kernel/locking/lockdep.c:238 at __lock_acquire+0x39d/0x2cf0 kernel/locking/lockdep.c:5187, CPU#0: syz.0.8675/6349 Modules linked in: CPU: 0 UID: 0 PID: 6349 Comm: syz.0.8675 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/13/2026 RIP: 0010:hlock_class kernel/locking/lockdep.c:238 [inline] RIP: 0010:check_wait_context kernel/locking/lockdep.c:4854 [inline] RIP: 0010:__lock_acquire+0x3a4/0x2cf0 kernel/locking/lockdep.c:5187 Code: 18 00 4c 8b 74 24 08 75 27 90 e8 17 f2 fc 02 85 c0 74 1c 83 3d 50 e0 4e 0e 00 75 13 48 8d 3d 43 f7 51 0e 48 c7 c6 8b 3a de 8d <67> 48 0f b9 3a 90 31 c0 0f b6 98 c4 00 00 00 41 8b 45 20 25 ff 1f RSP: 0018:ffffc9000c767680 EFLAGS: 00010046 RAX: 0000000000000001 RBX: 0000000000040000 RCX: 0000000000080000 RDX: ffffc90013080000 RSI: ffffffff8dde3a8b RDI: ffffffff8ff24ca0 RBP: 0000000000000003 R08: ffffffff8fef35a3 R09: 1ffffffff1fde6b4 R10: dfffffc0000000000 R11: fffffbfff1fde6b5 R12: 00000000000012a2 R13: ffff888030338ba8 R14: ffff888030338000 R15: ffff888030338b30 FS: 00007fa5995f66c0(0000) GS:ffff8881256f8000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f7e72f842d0 CR3: 00000000485a0000 CR4: 00000000003526f0 Call Trace: <TASK> lock_acquire+0x106/0x330 kernel/locking/lockdep.c:5868 touch_wq_lockdep_map+0xcb/0x180 kernel/workqueue.c:3940 __flush_workqueue+0x14b/0x14f0 kernel/workqueue.c:3982 nci_close_device+0x302/0x630 net/nfc/nci/core.c:567 nci_dev_down+0x3b/0x50 net/nfc/nci/core.c:639 nfc_dev_down+0x152/0x290 net/nfc/core.c:161 nfc_rfkill_set_block+0x2d/0x100 net/nfc/core.c:179 rfkill_set_block+0x1d2/0x440 net/rfkill/core.c:346 rfkill_fop_write+0x461/0x5a0 net/rfkill/core.c:1301 vfs_write+0x29a/0xb90 fs/read_write.c:684 ksys_write+0x150/0x270 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe2/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fa59b39acb9 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fa5995f6028 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00007fa59b615fa0 RCX: 00007fa59b39acb9 RDX: 0000000000000008 RSI: 0000200000000080 RDI: 0000000000000007 RBP: 00007fa59b408bf7 R08: ---truncated---	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: ice: Fix NULL pointer dereference in ice_vsi_set_napi_queues Add NULL pointer checks in ice_vsi_set_napi_queues() to prevent crashes during resume from suspend when rings[q_idx]->q_vector is NULL. Tested adaptor: 60:00.0 Ethernet controller [0200]: Intel Corporation Ethernet Controller E810-XXV for SFP [8086:159b] (rev 02) Subsystem: Intel Corporation Ethernet Network Adapter E810-XXV-2 [8086:4003] SR-IOV state: both disabled and enabled can reproduce this issue. kernel version: v6.18 Reproduce steps: Boot up and execute suspend like systemctl suspend or rtcwake. Log: <1>[231.443607] BUG: kernel NULL pointer dereference, address: 0000000000000040 <1>[231.444052] #PF: supervisor read access in kernel mode <1>[231.444484] #PF: error_code(0x0000) - not-present page <6>[231.444913] PGD 0 P4D 0 <4>[231.445342] Oops: Oops: 0000 [#1] SMP NOPTI <4>[231.446635] RIP: 0010:netif_queue_set_napi+0xa/0x170 <4>[231.447067] Code: 31 f6 31 ff c3 cc cc cc cc 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 0f 1f 44 00 00 48 85 c9 74 0b <48> 83 79 30 00 0f 84 39 01 00 00 55 41 89 d1 49 89 f8 89 f2 48 89 <4>[231.447513] RSP: 0018:ffffcc780fc078c0 EFLAGS: 00010202 <4>[231.447961] RAX: ffff8b848ca30400 RBX: ffff8b848caf2028 RCX: 0000000000000010 <4>[231.448443] RDX: 0000000000000000 RSI: 0000000000000000 RDI:		

2026-23166	ffff8b848dbd4000 <4>[231.448896] RBP: ffffcc780fc078e8 R08: 0000000000000000 R09: 0000000000000000 <4>[231.449345] R10: 0000000000000000 R11: 0000000000000000 R12: 0000000000000001 <4>[231.449817] R13: ffff8b848dbd4000 R14: ffff8b84833390c8 R15: 0000000000000000 <4>[231.450265] FS: 00007c7b29e9d740(0000) GS:ffff8b8c068e2000(0000) knlGS:0000000000000000 <4>[231.450715] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 <4>[231.451179] CR2: 0000000000000040 CR3: 000000030626f004 CR4: 0000000000f72ef0 <4>[231.451629] PKRU: 55555554 <4>[231.452076] Call Trace: <4>[231.452549] <TASK> <4>[231.452996] ? ice_vsi_set_napi_queues+0x4d/0x110 [ice] <4>[231.453482] ice_resume+0xfd/0x220 [ice] <4>[231.453977] ? __pfx_pci_pm_resume+0x10/0x10 <4>[231.454425] pci_pm_resume+0x8c/0x140 <4>[231.454872] ? __pfx_pci_pm_resume+0x10/0x10 <4>[231.455347] dpm_run_callback+0x5f/0x160 <4>[231.455796] ? dpm_wait_for_superior+0x107/0x170 <4>[231.456244] device_resume+0x177/0x270 <4>[231.456708] dpm_resume+0x209/0x2f0 <4>[231.457151] dpm_resume_end+0x15/0x30 <4>[231.457596] suspend_devices_and_enter+0x1da/0x2b0 <4>[231.458054] enter_state+0x10e/0x570 Add defensive checks for both the ring pointer and its q_vector before dereferencing, allowing the system to resume successfully even when q_vectors are unmapped.	N/A	More Details
CVE-2026-23165	In the Linux kernel, the following vulnerability has been resolved: sfc: fix deadlock in RSS config read Since cited commit, core locks the net_device's rss_lock when handling ethtool -x command, so driver's implementation should not lock it again. Remove the latter.	N/A	More Details
CVE-2026-23164	In the Linux kernel, the following vulnerability has been resolved: rocker: fix memory leak in rocker_world_port_post_fini() In rocker_world_port_pre_init(), rocker_port->wpriv is allocated with kzalloc(wops->port_priv_size, GFP_KERNEL). However, in rocker_world_port_post_fini(), the memory is only freed when wops->port_post_fini callback is set: if (!wops->port_post_fini) return; wops->port_post_fini(rocker_port); kfree(rocker_port->wpriv); Since rocker_ofdpa_ops does not implement port_post_fini callback (it is NULL), the wpriv memory allocated for each port is never freed when ports are removed. This leads to a memory leak of sizeof(struct ofdpa_port) bytes per port on every device removal. Fix this by always calling kfree(rocker_port->wpriv) regardless of whether the port_post_fini callback exists.	N/A	More Details
CVE-2026-23163	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix NULL pointer dereference in amdgpu_gmc_filter_faults_remove On APUs such as Raven and Renoir (GC 9.1.0, 9.2.2, 9.3.0), the ih1 and ih2 interrupt ring buffers are not initialized. This is by design, as these secondary IH rings are only available on discrete GPUs. See vega10_ih_sw_init() which explicitly skips ih1/ih2 initialization when AMD_IS_APU is set. However, amdgpu_gmc_filter_faults_remove() unconditionally uses ih1 to get the timestamp of the last interrupt entry. When retry faults are enabled on APUs (noretry=0), this function is called from the SVM page fault recovery path, resulting in a NULL pointer dereference when amdgpu_ih_decode_iv_ts_helper() attempts to access ih->ring[]. The crash manifests as: BUG: kernel NULL pointer dereference, address: 0000000000000004 RIP: 0010:amdgpu_ih_decode_iv_ts_helper+0x22/0x40 [amdgpu] Call Trace: amdgpu_gmc_filter_faults_remove+0x60/0x130 [amdgpu] svm_range_restore_pages+0xae5/0x11c0 [amdgpu] amdgpu_vm_handle_fault+0xc8/0x340 [amdgpu] gmc_v9_0_process_interrupt+0x191/0x220 [amdgpu] amdgpu_irq_dispatch+0xed/0x2c0 [amdgpu] amdgpu_ih_process+0x84/0x100 [amdgpu] This issue was exposed by commit 1446226d32a4 ("drm/amdgpu: Remove GC HW IP 9.3.0 from noretry=1") which changed the default for Renoir APU from noretry=1 to noretry=0, enabling retry fault handling and thus exercising the buggy code path. Fix this by adding a check for ih1.ring_size before attempting to use it. Also restore the soft_ih support from commit dd299441654f ("drm/amdgpu: Rework retry fault removal"). This is needed if the hardware doesn't support secondary HW IH rings. v2: additional updates (Alex) (cherry picked from commit 6ce8d536c80aa1f059e82184f0d1994436b1d526)	N/A	More Details
CVE-2026-23161	In the Linux kernel, the following vulnerability has been resolved: mm/shmem, swap: fix race of truncate and swap entry split The helper for shmem swap freeing is not handling the order of swap entries correctly. It uses xa_cmpxchg_irq to erase the swap entry, but it gets the entry order before that using xa_get_order without lock protection, and it may get an outdated order value if the entry is split or changed in other ways after the xa_get_order and before the xa_cmpxchg_irq. And besides, the order could grow and be larger than expected, and cause truncation to erase data beyond the end border. For example, if the target entry and following entries are swapped in or freed, then a large folio was added in place and swapped out, using the same entry, the xa_cmpxchg_irq will still succeed, it's very unlikely to happen though. To fix that, open code the Xarray cmpxchg and put the order retrieval and value checking in the same critical section. Also, ensure the order won't exceed the end border, skip it if the entry goes across the border. Skipping large swap entries crosses the end border is safe here. Shmem truncate iterates the range twice, in the first iteration, find_lock_entries already filtered such entries, and shmem will swapin the entries that cross the end border and partially truncate the folio (split the folio or at least zero part of it). So in the second loop here, if we see a swap entry that crosses the end order, it must at least have its content erased already. I observed random swapoff hangs and kernel panics when stress testing ZSWAP with shmem. After applying this patch, all problems are gone.	N/A	More Details
CVE-2026-23148	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix race in nvmet_bio_done() leading to NULL pointer dereference There is a race condition in nvmet_bio_done() that can cause a NULL pointer dereference in blk_cgroup_bio_start(): 1. nvmet_bio_done() is called when a bio completes 2. nvmet_req_complete() is called, which invokes req->ops->queue_response(req) 3. The queue_response callback can re-queue and re-submit the same request 4. The re-submission reuses the same inline_bio from nvmet_req 5. Meanwhile, nvmet_req_bio_put() (called after nvmet_req_complete) invokes bio_uninit() for inline_bio, which sets bio->bi_blkg to NULL 6. The re-submitted bio enters submit_bio_noacct_nocheck() 7. blk_cgroup_bio_start() dereferences bio->bi_blkg, causing a crash: BUG: kernel NULL pointer dereference, address: 0000000000000028 #PF: supervisor read access in kernel mode RIP: 0010:blk_cgroup_bio_start+0x10/0xd0 Call Trace: submit_bio_noacct_nocheck+0x44/0x250 nvmet_bdev_execute_rw+0x254/0x370 [nvmet] process_one_work+0x193/0x3c0 worker_thread+0x281/0x3a0 Fix this by reordering nvmet_bio_done() to call nvmet_req_bio_put() BEFORE nvmet_req_complete(). This ensures the bio is cleaned up before the request can be re-submitted, preventing the race condition.	N/A	More Details
CVE-2026-23160	In the Linux kernel, the following vulnerability has been resolved: octeon_ep: Fix memory leak in octep_device_setup() In octep_device_setup(), if octep_ctrl_net_init() fails, the function returns directly without unmapping the mapped resources and freeing the allocated configuration memory. Fix this by jumping to the unsupported_dev label, which performs the necessary cleanup. This aligns with the error handling logic of other paths in this function. Compile tested only. Issue found using a prototype static analysis tool and code review.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: perf: sched: Fix perf crash with new is_user_task() helper In order to do a user space stacktrace the current task needs to be a user task that has executed in user space. It use to be possible to test if a task is a user task or not by simply checking the task_struct mm field. If it was non NULL, it was a user task		

CVE-2026-23159	and if not it was a kernel task. But things have changed over time, and some kernel tasks now have their own mm field. An idea was made to instead test PF_KTHREAD and two functions were used to wrap this check in case it became more complex to test if a task was a user task or not[1]. But this was rejected and the C code simply checked the PF_KTHREAD directly. It was later found that not all kernel threads set PF_KTHREAD. The io-uring helpers instead set PF_USER_WORKER and this needed to be added as well. But checking the flags is still not enough. There's a very small window when a task exits that it frees its mm field and it is set back to NULL. If perf were to trigger at this moment, the flags test would say its a user space task but when perf would read the mm field it would crash with at NULL pointer dereference. Now there are flags that can be used to test if a task is exiting, but they are set in areas that perf may still want to profile the user space task (to see where it exited). The only real test is to check both the flags and the mm field. Instead of making this modification in every location, create a new is_user_task() helper function that does all the tests needed to know if it is safe to read the user space memory or not. [1] https://lore.kernel.org/all/20250425204120.639530125@goodmis.org/	N/A	More Details
CVE-2026-23158	In the Linux kernel, the following vulnerability has been resolved: gpio: virtuser: fix UAF in configfs release path The gpio-virtuser configfs release path uses guard(mutex) to protect the device structure. However, the device is freed before the guard cleanup runs, causing mutex_unlock() to operate on freed memory. Specifically, gpio_virtuser_device_config_group_release() destroys the mutex and frees the device while still inside the guard(mutex) scope. When the function returns, the guard cleanup invokes mutex_unlock(&dev->lock), resulting in a slab use-after-free. Limit the mutex lifetime by using a scoped_guard() only around the activation check, so that the lock is released before mutex_destroy() and kfree() are called.	N/A	More Details
CVE-2026-23157	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not strictly require dirty metadata threshold for metadata writepages [BUG] There is an internal report that over 1000 processes are waiting at the io_schedule_timeout() of balance_dirty_pages(), causing a system hang and trigger a kernel coredump. The kernel is v6.4 kernel based, but the root problem still applies to any upstream kernel before v6.18. [CAUSE] From Jan Kara for his wisdom on the dirty page balance behavior first. This cgroup dirty limit was what was actually playing the role here because the cgroup had only a small amount of memory and so the dirty limit for it was something like 16MB. Dirty throttling is responsible for enforcing that nobody can dirty (significantly) more dirty memory than there's dirty limit. Thus when a task is dirtying pages it periodically enters into balance_dirty_pages() and we let it sleep there to slow down the dirtying. When the system is over dirty limit already (either globally or within a cgroup of the running task), we will not let the task exit from balance_dirty_pages() until the number of dirty pages drops below the limit. So in this particular case, as I already mentioned, there was a cgroup with relatively small amount of memory and as a result with dirty limit set at 16MB. A task from that cgroup has dirtied about 28MB worth of pages in btrfs btree inode and these were practically the only dirty pages in that cgroup. So that means the only way to reduce the dirty pages of that cgroup is to writeback the dirty pages of btrfs btree inode, and only after that those processes can exit balance_dirty_pages(). Now back to the btrfs part, btree_writepages() is responsible for writing back dirty btree inode pages. The problem here is, there is a btrfs internal threshold that if the btree inode's dirty bytes are below the 32M threshold, it will not do any writeback. This behavior is to batch as much metadata as possible so we won't write back those tree blocks and then later re-COW them again for another modification. This internal 32MiB is higher than the existing dirty page size (28MiB), meaning no writeback will happen, causing a deadlock between btrfs and cgroup: - Btrfs doesn't want to write back btree inode until more dirty pages - Cgroup/MM doesn't want more dirty pages for btrfs btree inode Thus any process touching that btree inode is put into sleep until the number of dirty pages is reduced. Thanks Jan Kara a lot for the analysis of the root cause. [ENHANCEMENT] Since kernel commit b55102826d7d ("btrfs: set AS_KERNEL_FILE on the btree_inode"), btrfs btree inode pages will only be charged to the root cgroup which should have a much larger limit than btrfs' 32MiB threshold. So it should not affect newer kernels. But for all current LTS kernels, they are all affected by this problem, and backporting the whole AS_KERNEL_FILE may not be a good idea. Even for newer kernels I still think it's a good idea to get rid of the internal threshold at btree_writepages(), since for most cases cgroup/MM has a better view of full system memory usage than btrfs' fixed threshold. For internal callers using btrfs_btree_balance_dirty() since that function is already doing internal threshold check, we don't need to bother them. But for external callers of btree_writepages(), just respect their requests and write back whatever they want, ignoring the internal btrfs threshold to avoid such deadlock on btree inode dirty page balancing.	N/A	More Details
CVE-2026-23156	In the Linux kernel, the following vulnerability has been resolved: efivarfs: fix error propagation in efivar_entry_get() efivar_entry_get() always returns success even if the underlying __efivar_entry_get() fails, masking errors. This may result in uninitialized heap memory being copied to userspace in the efivarfs_file_read() path. Fix it by returning the error from __efivar_entry_get().	N/A	More Details
CVE-2026-23155	In the Linux kernel, the following vulnerability has been resolved: can: gs_usb: gs_usb_receive_bulk_callback(): fix error message Sinc commit 79a6d1bfe114 ("can: gs_usb: gs_usb_receive_bulk_callback(): unanchor URL on usb_submit_urb() error") a failing resubmit URB will print an info message. In the case of a short read where netdev has not yet been assigned, initialize as NULL to avoid dereferencing an undefined value. Also report the error value of the failed resubmit.	N/A	More Details
CVE-2026-23154	In the Linux kernel, the following vulnerability has been resolved: net: fix segmentation of forwarding fraglist GRO This patch enhances GSO segment handling by properly checking the SKB_GSO_DODGY flag for frag_list GSO packets, addressing low throughput issues observed when a station accesses IPv4 servers via hotspots with an IPv6-only upstream interface. Specifically, it fixes a bug in GSO segmentation when forwarding GRO packets containing a frag_list. The function skb_segment_list cannot correctly process GRO skbs that have been converted by XLAT, since XLAT only translates the header of the head skb. Consequently, skbs in the frag_list may remain untranslated, resulting in protocol inconsistencies and reduced throughput. To address this, the patch explicitly sets the SKB_GSO_DODGY flag for GSO packets in XLAT's IPv4/IPv6 protocol translation helpers (bpf_skb_proto_4_to_6 and bpf_skb_proto_6_to_4). This marks GSO packets as potentially modified after protocol translation. As a result, GSO segmentation will avoid using skb_segment_list and instead falls back to skb_segment for packets with the SKB_GSO_DODGY flag. This ensures that only safe and fully translated frag_list packets are processed by skb_segment_list, resolving protocol inconsistencies and improving throughput when forwarding GRO packets converted by XLAT.	N/A	More Details
CVE-2026-23153	In the Linux kernel, the following vulnerability has been resolved: firewire: core: fix race condition against transaction list The list of transaction is enumerated without acquiring card lock when processing AR response event. This causes a race condition bug when processing AT request completion event concurrently. This commit fixes the bug by put timer start for split transaction expiration into the scope of lock. The value of jiffies in card structure is referred before acquiring the lock.	N/A	More Details
CVE-2026-23152	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: correctly decode TTLM with default link map TID-To-Link Mapping (TTLM) elements do not contain any link mapping presence indicator if a default mapping is used and parsing needs to be skipped. Note that access points should not explicitly report an advertised TTLM with a default mapping as that is the implied mapping if the element is not included, this is even the case when switching back to the default mapping.	N/A	More Details

	However, mac80211 would incorrectly parse the frame and would also read one byte beyond the end of the element.		
CVE-2026-23151	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix memory leak in set_ssp_complete Fix memory leak in set_ssp_complete() where mgmt_pending_cmd structures are not freed after being removed from the pending list. Commit 302a1f674c00 ("Bluetooth: MGMT: Fix possible UAFs") replaced mgmt_pending_foreach() calls with individual command handling but missed adding mgmt_pending_free() calls in both error and success paths of set_ssp_complete(). Other completion functions like set_le_complete() were fixed correctly in the same commit. This causes a memory leak of the mgmt_pending_cmd structure and its associated parameter data for each SSP command that completes. Add the missing mgmt_pending_free(cmd) calls in both code paths to fix the memory leak. Also fix the same issue in set_advertising_complete().	N/A	More Details
CVE-2026-23150	In the Linux kernel, the following vulnerability has been resolved: nfc: llcp: Fix memleak in nfc_llcp_send_ui_frame(). syzbot reported various memory leaks related to NFC, struct nfc_llcp_sock, sk_buff, nfc_dev, etc. [0] The leading log hinted that nfc_llcp_send_ui_frame() failed to allocate skb due to sock_error(sk) being -ENXIO. ENXIO is set by nfc_llcp_socket_release() when struct nfc_llcp_local is destroyed by local_cleanup(). The problem is that there is no synchronisation between nfc_llcp_send_ui_frame() and local_cleanup(), and skb could be put into local->tx_queue after it was purged in local_cleanup(): CPU1 CPU2 ---- ---- nfc_llcp_send_ui_frame() local_cleanup() |- do { ' |- pdu = nfc_alloc_send_skb(..., &err) | . | |- nfc_llcp_socket_release(local, false, ENXIO); | |- skb_queue_purge(&local->tx_queue); | | ' | |- skb_queue_tail(&local->tx_queue, pdu); | ... | |- pdu = nfc_alloc_send_skb(..., &err) | ^._____.' local_cleanup() is called for struct nfc_llcp_local only after nfc_llcp_remove_local() unlinks it from llcp_devices. If we hold local->tx_queue.lock then, we can synchronise the thread and nfc_llcp_send_ui_frame(). Let's do that and check list_empty(&local->list) before queuing skb to local->tx_queue in nfc_llcp_send_ui_frame(). [0]: [56.074943][T6096] llcp: nfc_llcp_send_ui_frame: Could not allocate PDU (error=-6) [64.318868][T5813] kmemleak: 6 new suspected memory leaks (see /sys/kernel/debug/kmemleak) BUG: memory leak unreferenced object 0xffff8881272f6800 (size 1024): comm "syz.0.17", pid 6096, jiffies 4294942766 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 27 00 03 40 00 00 00 00 00 00 00 00 00 00 00 00 '..@..... backtrace (crc da58d84d): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4979 [inline] slab_alloc_node mm/slub.c:5284 [inline] __do_kmalloc_node mm/slub.c:5645 [inline] __kmalloc_noprof+0x3e3/0x6b0 mm/slub.c:5658 kmalloc_noprof include/linux/slab.h:961 [inline] sk_prot_alloc+0x11a/0x1b0 net/core/sock.c:2239 sk_alloc+0x36/0x360 net/core/sock.c:2295 nfc_llcp_sock_alloc+0x37/0x130 net/nfc/llcp_sock.c:979 llcp_sock_create+0x71/0xd0 net/nfc/llcp_sock.c:1044 nfc_sock_create+0xc9/0xf0 net/nfc/af_nfc.c:31 __sock_create+0x1a9/0x340 net/socket.c:1605 sock_create net/socket.c:1663 [inline] __sys_socket_create net/socket.c:1700 [inline] __sys_socket+0xb9/0x1a0 net/socket.c:1747 __do_sys_socket net/socket.c:1761 [inline] __se_sys_socket net/socket.c:1759 [inline] __x64_sys_socket+0x1b/0x30 net/socket.c:1759 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xa4/0xfa0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f BUG: memory leak unreferenced object 0xffff88810fbd9800 (size 240): comm "syz.0.17", pid 6096, jiffies 4294942850 hex dump (first 32 bytes): 68 f0 ff 08 81 88 ff ff 68 f0 ff 08 81 88 ff ff h.....h..... 00 00 00 00 00 00 00 00 68 2f 27 81 88 ff ff ..... backtrace (crc 6cc652b1): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4979 [inline] slab_alloc_node mm/slub.c:5284 [inline] kmem_cache_alloc_node_noprof+0x36f/0x5e0 mm/slub.c:5336 __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/sk ---truncated---	N/A	More Details
CVE-2026-23149	In the Linux kernel, the following vulnerability has been resolved: drm: Do not allow userspace to trigger kernel warnings in drm_gem_change_handle_ioctl() Since GEM bo handles are u32 in the uapi and the internal implementation uses idr_alloc() which uses int ranges, passing a new handle larger than INT_MAX trivially triggers a kernel warning: idr_alloc(): ... if (WARN_ON_ONCE(start < 0)) return -EINVAL; ... Fix it by rejecting new handles above INT_MAX and at the same time make the end limit calculation more obvious by moving into int domain.	N/A	More Details
CVE-2026-23119	In the Linux kernel, the following vulnerability has been resolved: bonding: provide a net pointer to __skb_flow_dissect() After 3cbf4ffba5ee ("net: plumb network namespace into __skb_flow_dissect") we have to provide a net pointer to __skb_flow_dissect(), either via skb->dev, skb->sk, or a user provided pointer. In the following case, syzbot was able to cook a bare skb. WARNING: net/core/flow_dissector.c:1131 at __skb_flow_dissect+0xb57/0x68b0 net/core/flow_dissector.c:1131, CPU#1: syz.2.1418/11053 Call Trace: <TASK> bond_flow_dissect drivers/net/bonding/bond_main.c:4093 [inline] __bond_xmit_hash+0x2d7/0xba0 drivers/net/bonding/bond_main.c:4157 bond_xmit_hash_xdp drivers/net/bonding/bond_main.c:4208 [inline] bond_xdp_xmit_3ad_xor_slave_get drivers/net/bonding/bond_main.c:5139 [inline] bond_xdp_get_xmit_slave+0x1fd/0x710 drivers/net/bonding/bond_main.c:5515 xdp_master_redirect+0x13f/0x2c0 net/core/filter.c:4388 bpf_prog_run_xdp include/net/xdp.h:700 [inline] bpf_test_run+0x6b2/0x7d0 net/bpf/test_run.c:421 bpf_prog_test_run_xdp+0x795/0x10e0 net/bpf/test_run.c:1390 bpf_prog_test_run+0x2c7/0x340 kernel/bpf/syscall.c:4703 __sys_bpf+0x562/0x860 kernel/bpf/syscall.c:6182 __do_sys_bpf kernel/bpf/syscall.c:6274 [inline] __se_sys_bpf kernel/bpf/syscall.c:6272 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:6272 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xec/0xf80 arch/x86/entry/syscall_64.c:94	N/A	More Details
CVE-2026-23118	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix data-race warning and potential load/store tearing Fix the following: BUG: KCSAN: data-race in rxrpc_peer_keepalive_worker / rxrpc_send_data_packet which is reporting an issue with the reads and writes to ->last_tx_at in: conn->peer->last_tx_at = ktime_get_seconds(); and: keepalive_at = peer->last_tx_at + RXRPC_KEEPALIVE_TIME; The lockless accesses to these to values aren't actually a problem as the read only needs an approximate time of last transmission for the purposes of deciding whether or not the transmission of a keepalive packet is warranted yet. Also, as ->last_tx_at is a 64-bit value, tearing can occur on a 32-bit arch. Fix both of these by switching to an unsigned int for ->last_tx_at and only storing the LSW of the time64_t. It can then be reconstructed at need provided no more than 68 years has elapsed since the last transmission.	N/A	More Details
CVE-2026-23117	In the Linux kernel, the following vulnerability has been resolved: ice: add missing ice_deinit_hw() in devlink reinit path devlink-reload results in ice_init_hw failed error, and then removing the ice driver causes a NULL pointer dereference. [+0.102213] ice 0000:ca:00.0: ice_init_hw failed: -16 ... [+0.000001] Call Trace: [+0.000003] <TASK> [+0.000006] ice_unload+0x8f/0x100 [ice] [+0.000081] ice_remove+0xba/0x300 [ice] Commit 1390b8b3d2be ("ice: remove duplicate call to ice_deinit_hw() on error paths") removed ice_deinit_hw() from ice_deinit_dev(). As a result ice_devlink_reinit_down() no longer calls ice_deinit_hw(), but ice_devlink_reinit_up() still calls ice_init_hw(). Since the control queues are not uninitialized, ice_init_hw() fails with -EBUSY. Add ice_deinit_hw() to ice_devlink_reinit_down() to correspond with ice_init_hw() in ice_devlink_reinit_up().	N/A	More Details
CVE-2025-35993	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2026-26264	BACnet Stack is a BACnet open source protocol stack C library for embedded systems. Prior to 1.5.0rc4 and 1.4.3rc2, a malformed WriteProperty request can trigger a length underflow in the BACnet stack, leading to an out-of-bounds read and a crash (DoS). The issue is in wp.c within wp_decode_service_request. When decoding the optional priority context tag, the code passes apdu_len - apdu_size to bacnet_unsigned_context_decode without validating that apdu_size <= apdu_len. If a truncated APDU reaches this path, apdu_len - apdu_size underflows, resulting in a large size being used for decoding and an out-of-bounds read. This vulnerability is fixed in 1.5.0rc4 and 1.4.3rc2.	N/A	More Details
CVE-2025-36552	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36545	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36542	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36538	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36534	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36532	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36526	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36524	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36523	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-36517	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-35997	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-35976	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2024-34154	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-35962	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-35961	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-35960	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-32734	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-32733	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

32090			
CVE-2025-32085	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-32082	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-32009	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-31942	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-31364	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2025-31358	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45291	Rejected reason: reserved but not needed	N/A	More Details
CVE-2024-34157	Rejected reason: reserved but not needed	N/A	More Details
CVE-2026-23116	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx8m-blk-ctrl: Remove separate rst and clk mask for 8mq vpu For i.MX8MQ platform, the ADB in the VPUMIX domain has no separate reset and clock enable bits, but is ungated and reset together with the VPUs. So we can't reset G1 or G2 separately, it may led to the system hang. Remove rst_mask and clk_mask of imx8mq_vpu_blk_ctl_domain_data. Let imx8mq_vpu_power_notifier() do really vpu reset.	N/A	More Details
CVE-2026-26295	Rejected reason: Not used	N/A	More Details
CVE-2026-23115	In the Linux kernel, the following vulnerability has been resolved: serial: Fix not set tty->port race condition Revert commit bfc467db60b7 ("serial: remove redundant tty_port_link_device()") because the tty_port_link_device() is not redundant: the tty->port has to be confured before we call uart_configure_port(), otherwise user-space can open console without TTY linked to the driver. This tty_port_link_device() was added explicitly to avoid this exact issue in commit fb2b90014d78 ("tty: link tty and port before configuring it as console"), so offending commit basically reverted the fix saying it is redundant without addressing the actual race condition presented there. Reproducible always as tty->port warning on Qualcomm SoC with most of devices disabled, so with very fast boot, and one serial device being the console: printk: legacy console [ttyMSM0] enabled printk: legacy console [ttyMSM0] enabled printk: legacy bootconsole [qcom_geni0] disabled printk: legacy bootconsole [qcom_geni0] disabled ------------[cut here]------------ tty_init_dev: ttyMSM driver does not set tty->port. This would crash the kernel. Fix the driver! WARNING: drivers/tty/tty_io.c:1414 at tty_init_dev.part.0+0x228/0x25c, CPU#2: systemd/1 Modules linked in: socinfo tcsrcc_eliza gcc_eliza sm3_ce fuse ipv6 CPU: 2 UID: 0 PID: 1 Comm: systemd Tainted: G S 6.19.0-rc4-next-20260108-00024-g2202f4d30aa8 #73 PREEMPT Tainted: [S]=CPU_OUT_OF_SPEC Hardware name: Qualcomm Technologies, Inc. Eliza (DT) ... tty_init_dev.part.0 (drivers/tty/tty_io.c:1414 (discriminator 11)) (P) tty_open (arch/arm64/include/asm/atomic_ll_sc.h:95 (discriminator 3) drivers/tty/tty_io.c:2073 (discriminator 3) drivers/tty/tty_io.c:2120 (discriminator 3)) chrdev_open (fs/char_dev.c:411) do_dentry_open (fs/open.c:962) vfs_open (fs/open.c:1094) do_open (fs/namei.c:4634) path_openat (fs/namei.c:4793) do_filp_open (fs/namei.c:4820) do_sys_openat2 (fs/open.c:1391 (discriminator 3)) ... Starting Network Name Resolution... Apparently the flow with this small Yocto-based ramdisk user-space is: driver (qcom_geni_serial.c): user-space: ========== ========== qcom_geni_serial_probe() uart_add_one_port() serial_core_register_port() serial_core_add_one_port() uart_configure_port() register_console() | | open console | ... | tty_init_dev() | driver->ports[idx] is NULL | tty_port_register_device_attr_serdev() tty_port_link_device() <- set driver->ports[idx]	N/A	More Details
CVE-2026-23114	In the Linux kernel, the following vulnerability has been resolved: arm64/fpsimd: ptrace: Fix SVE writes on !SME systems When SVE is supported but SME is not supported, a ptrace write to the NT_ARM_SVE regset can place the tracee into an invalid state where (non-streaming) SVE register data is stored in FP_STATE_SVE format but TIF_SVE is clear. This can result in a later warning from fpsimd_restore_current_state(), e.g. WARNING: CPU: 0 PID: 7214 at arch/arm64/kernel/fpsimd.c:383 fpsimd_restore_current_state+0x50c/0x748 When this happens, fpsimd_restore_current_state() will set TIF_SVE, placing the task into the correct state. This occurs before any other check of TIF_SVE can possibly occur, as other checks of TIF_SVE only happen while the FPSIMD/SVE/SME state is live. Thus, aside from the warning, there is no functional issue. This bug was introduced during rework to error handling in commit: 9f8bf718f2923 ("arm64/fpsimd: ptrace: Gracefully handle errors") ... where the setting of TIF_SVE was moved into a block which is only executed when system_supports_sme() is true. Fix this by removing the system_supports_sme() check. This ensures that TIF_SVE is set for (SVE-formatted) writes to NT_ARM_SVE, at the cost of unconditionally manipulating the tracee's saved svcr value. The manipulation of svcr is benign and inexpensive, and we already do similar elsewhere (e.g. during signal handling), so I don't think it's worth guarding this with system_supports_sme() checks. Aside from the above, there is no functional change. The 'type' argument to sve_set_common() is only set to ARM64_VEC_SME (in ssve_set())) when system_supports_sme(), so the ARM64_VEC_SME case in the switch statement is still unreachable when !system_supports_sme(). When CONFIG_ARM64_SME=n, the only caller of sve_set_common() is sve_set(), and the compiler can constant-fold for the case where type is ARM64_VEC_SVE, removing the logic for other cases.	N/A	More Details

CVE-2026-23113	In the Linux kernel, the following vulnerability has been resolved: io_uring/io-wq: check IO_WQ_BIT_EXIT inside work run loop Currently this is checked before running the pending work. Normally this is quite fine, as work items either end up blocking (which will create a new worker for other items), or they complete fairly quickly. But syzbot reports an issue where io-wq takes seemingly forever to exit, and with a bit of debugging, this turns out to be because it queues a bunch of big (2GB - 4096b) reads with a /dev/msr* file. Since this file type doesn't support ->read_iter(), loop_rw_iter() ends up handling them. Each read returns 16MB of data read, which takes 20 (!!) seconds. With a bunch of these pending, processing the whole chain can take a long time. Easily longer than the syzbot uninterruptible sleep timeout of 140 seconds. This then triggers a complaint off the io-wq exit path: INFO: task syz.4.135:6326 blocked for more than 143 seconds. Not tainted syzkaller #0 Blocked by coredump. "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:syz.4.135 state:D stack:26824 pid:6326 tgid:6324 ppid:5957 task_flags:0x400548 flags:0x00080000 Call Trace: <TASK> context_switch kernel/sched/core.c:5256 [inline] __schedule+0x1139/0x6150 kernel/sched/core.c:6863 __schedule_loop kernel/sched/core.c:6945 [inline] schedule+0xe7/0x3a0 kernel/sched/core.c:6960 schedule_timeout+0x257/0x290 kernel/time/sleep_timeout.c:75 do_wait_for_common kernel/sched/completion.c:100 [inline] __wait_for_common+0x2fc/0x4e0 kernel/sched/completion.c:121 io_wq_exit_workers io_uring/io-wq.c:1328 [inline] io_wq_put_and_exit+0x271/0x8a0 io_uring/io-wq.c:1356 io_uring_clean_tctx+0x10d/0x190 io_uring/tctx.c:203 io_uring_cancel_generic+0x69c/0x9a0 io_uring/cancel.c:651 io_uring_files_cancel include/linux/io_uring.h:19 [inline] do_exit+0x2ce/0x2bd0 kernel/exit.c:911 do_group_exit+0xd3/0x2a0 kernel/exit.c:1112 get_signal+0x2671/0x26d0 kernel/signal.c:3034 arch_do_signal_or_restart+0x8f/0x7e0 arch/x86/kernel/signal.c:337 __exit_to_user_mode_loop kernel/entry/common.c:41 [inline] exit_to_user_mode_loop+0x8c/0x540 kernel/entry/common.c:75 __exit_to_user_mode_prepare include/linux/irq-entry-common.h:226 [inline] syscall_exit_to_user_mode_prepare include/linux/irq-entry-common.h:256 [inline] syscall_exit_to_user_mode_work include/linux/entry-common.h:159 [inline] syscall_exit_to_user_mode include/linux/entry-common.h:194 [inline] do_syscall_64+0x4ee/0xf80 arch/x86/entry/syscall_64.c:100 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fa02738f749 RSP: 002b:00007fa0281ae0e8 EFLAGS: 00000246 ORIG_RAX: 00000000000000ca RAX: ffffffffffffffe00 RBX: 00007fa0275e6098 RCX: 00007fa02738f749 RDX: 0000000000000000 RSI: 0000000000000080 RDI: 00007fa0275e6098 RBP: 00007fa0275e6090 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fa0275e6128 R14: 00007fff14e4fcb0 R15: 00007fff14e4fd98 There's really nothing wrong here, outside of processing these reads will take a LONG time. However, we can speed up the exit by checking the IO_WQ_BIT_EXIT inside the io_worker_handle_work() loop, as syzbot will exit the ring after queueing up all of these reads. Then once the first item is processed, io-wq will simply cancel the rest. That should avoid syzbot running into this complaint again.	N/A	More Details
CVE-2025-71200	In the Linux kernel, the following vulnerability has been resolved: mmc: sdhci-of-dwcmshc: Prevent illegal clock reduction in HS200/HS400 mode When operating in HS200 or HS400 timing modes, reducing the clock frequency below 52MHz will lead to link broken as the Rockchip DWC MSHC controller requires maintaining a minimum clock of 52MHz in these modes. Add a check to prevent illegal clock reduction through debugfs: root@debian:/# echo 50000000 > /sys/kernel/debug/mmc0/clock root@debian:/# [30.090146] mmc0: running CQE recovery mmc0: cqhci: Failed to halt mmc0: cqhci: spurious TCN for tag 0 WARNING: drivers/mmc/host/cqhci-core.c:797 at cqhci_irq+0x254/0x818, CPU#1: kworker/1:0H/24 Modules linked in: CPU: 1 UID: 0 PID: 24 Comm: kworker/1:0H Not tainted 6.19.0-rc1-00001-g09db0998649d-dirty #204 PREEMPT Hardware name: Rockchip RK3588 EVB1 V10 Board (DT) Workqueue: kblockd blk_mq_run_work_fn pstate: 604000c9 (nZCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : cqhci_irq+0x254/0x818 lr : cqhci_irq+0x254/0x818 ...	N/A	More Details
CVE-2026-26303	Rejected reason: Not used	N/A	More Details
CVE-2026-26302	Rejected reason: Not used	N/A	More Details
CVE-2026-26301	Rejected reason: Not used	N/A	More Details
CVE-2026-26300	Rejected reason: Not used	N/A	More Details
CVE-2026-26299	Rejected reason: Not used	N/A	More Details
CVE-2026-26298	Rejected reason: Not used	N/A	More Details
CVE-2026-26297	Rejected reason: Not used	N/A	More Details
CVE-2026-26296	Rejected reason: Not used	N/A	More Details
CVE-2026-26273	Known is a social publishing platform. Prior to 1.6.3, a Critical Broken Authentication vulnerability exists in Known 1.6.2 and earlier. The application leaks the password reset token within a hidden HTML input field on the password reset page. This allows any unauthenticated attacker to retrieve the reset token for any user by simply querying the user's email, leading to full Account Takeover (ATO) without requiring access to the victim's email inbox. This vulnerability is fixed in 1.6.3.	N/A	More Details
CVE-2025-47915	Rejected reason: reserved but not needed	N/A	More Details

CVE-2025-70957	A Denial of Service (DoS) vulnerability was discovered in the TON Lite Server before v2024.09. The vulnerability arises from the handling of external arguments passed to locally executed "get methods." An attacker can inject a constructed Continuation object (an internal TVM type) that is normally restricted within the VM. When the TVM executes this malicious continuation, it consumes excessive CPU resources while accruing disproportionately low virtual gas costs. This "free" computation allows an attacker to monopolize the Lite Server's processing power, significantly reducing its throughput and causing a denial of service for legitimate users acting through the gateway.	N/A	More Details
CVE-2025-70955	A Stack Overflow vulnerability was discovered in the TON Virtual Machine (TVM) before v2024.10. The vulnerability stems from the improper handling of vmstate and continuation jump instructions, which allow for continuous dynamic tail calls. An attacker can exploit this by crafting a smart contract with deeply nested jump logic. Even within permissible gas limits, this nested execution exhausts the host process's stack space, causing the validator node to crash. This results in a Denial of Service (DoS) for the TON blockchain network.	N/A	More Details
CVE-2026-26335	Calero VeraSMART versions prior to 2022 R1 use static ASP.NET/IIS machineKey values configured for the VeraSMART web application and stored in C:\\Program Files (x86)\\Veramark\\VeraSMART\\WebRoot\\web.config. An attacker who obtains these keys can craft a valid ASP.NET ViewState payload that passes integrity validation and is accepted by the application, resulting in server-side deserialization and remote code execution in the context of the IIS application.	N/A	More Details
CVE-2026-26334	Calero VeraSMART versions prior to 2026 R1 contain hardcoded static AES encryption keys within Veramark.Framework.dll (Veramark.Core.Config class). These keys are used to encrypt the password of the service account stored in C:\\VeraSMART Data\\app.settings. An attacker with local access to the system can extract the hardcoded keys from the Veramark.Framework.dll module and decrypt the stored credentials. The recovered credentials can then be used to authenticate to the Windows host, potentially resulting in local privilege escalation depending on the privileges of the configured service account.	N/A	More Details
CVE-2026-26333	Calero VeraSMART versions prior to 2022 R1 expose an unauthenticated .NET Remoting HTTP service on TCP port 8001. The service publishes default ObjectURIs (including EndeavorServer.rem and RemoteFileReceiver.rem) and permits the use of SOAP and binary formatters with TypeFilterLevel set to Full. An unauthenticated remote attacker can invoke the exposed remoting endpoints to perform arbitrary file read and write operations via the WebClient class. This allows retrieval of sensitive files such as WebRoot\\web.config, which may disclose IIS machineKey validation and decryption keys. An attacker can use these keys to generate a malicious ASP.NET ViewState payload and achieve remote code execution within the IIS application context. Additionally, supplying a UNC path can trigger outbound SMB authentication from the service account, potentially exposing NTLMv2 hashes for relay or offline cracking.	N/A	More Details
CVE-2025-68128	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-68127	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-68126	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-68125	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-68124	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-58184	Rejected reason: reserved but not needed	N/A	More Details
CVE-2025-58182	Rejected reason: reserved but not needed	N/A	More Details
CVE-2026-2570	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