SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 June 2026

Generated on 10 June 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-2026-48303	Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
CVE-2026-47938	Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
CVE-2026-10520	An OS Command Injection vulnerability in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated user to achieve root-level remote code execution	10.0	More Details
CVE-2026-46389	UDS Identity Config builds the Keycloak configuration image (realm, plugins, theme, truststore, JARs) consumed by UDS Core's Identity deployment. In versions 0.11.0 through 0.26.0, a logic error in the `client-kubernetes-secret` Keycloak client authenticator (shipped by `uds-identity-config` and consumed by UDS Core) causes the submitted `client_secret` to be overwritten with the mounted Kubernetes secret before comparison. An attacker who can reach the Keycloak token endpoint and knows a `client_id` using this authenticator can authenticate as that client with any `client_secret` value and obtain OAuth2 tokens scoped to the client's service account. In the case of the `uds-operator` client this token can be used to registry/modify other clients. Version 0.26.1 patches the issue.	10.0	More Details
CVE-2026-49777	Improper Validation of Specified Quantity in Input vulnerability in ShapedPlugin, LLC Product Slider Pro for WooCommerce allows Malicious Software Implanted. This issue affects Product Slider Pro for WooCommerce: from n/a before 3.5.4.	10.0	More Details
CVE-2026-48567	Authentication bypass by spoofing in Azure HorizonDB allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-43986	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 expose a public `/image/<hash>` route that resolves attacker-controlled entries from `image_hash_lookup` and replays them through the same server-side image fetch logic used by authenticated image proxying. A low-privilege guest user can seed a malicious external image URL into this lookup table and then trigger server-side fetches through a fully unauthenticated endpoint. This turns an authenticated SSRF primitive into a persistent unauthenticated SSRF gadget. Once the	9.9	More Details

	malicious hash entry exists, any external user can request `/image/<hash>.png` and cause the PMS or Tautulli host to fetch an arbitrary attacker-chosen URL. Version 2.17.1 patches the issue.		
CVE-2026-10523	An Authentication Bypass vulnerability (CWE-288) in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated attacker to create arbitrary administrative accounts and obtain full administrative access	9.9	More Details
CVE-2026-44748	SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated attacker with normal privileges to obtain a valid signed message and send modified signed XML documents to the verifier. This may result in acceptance of tampered identity information leading to unauthorized access to sensitive user data and potential disruption of normal system usage. This causes a high impact on confidentiality, integrity and availability of the application.	9.9	More Details
CVE-2026-45744	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the GET /ssh/file_manager/ssh/resolvePath endpoint in Termix is vulnerable to OS command injection. The endpoint uses double-quote escaping for shell command construction, which does not prevent $(...) and backtick command substitution. Any authenticated user with an active File Manager SSH session can execute arbitrary commands on the connected remote host. Version 2.3.2 patches the issue.	9.9	More Details
CVE-2025-14771	Files or directories accessible to external parties vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	9.9	More Details
CVE-2026-41283	OpenStack Mistral through 22.0.0 allows Arbitrary Remote Code Execution when the API is exposed. There are endpoints that allow code execution, which can lead to exfiltration of service credentials.	9.9	More Details
CVE-2026-49188	The ai_cmd utility executes with full root permissions. It pipes socket inputs directly to popen(), paving the way for unauthenticated users to execute arbitrary root commands.	9.8	More Details
CVE-2024-58349	WordPress Theme Travelscape 1.0.3 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by exploiting insufficient validation in the theme's upload functionality. Attackers can upload arbitrary files to the theme directory and execute them to achieve remote code execution on the affected WordPress installation.	9.8	More Details
CVE-2026-25089	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox Cloud 5.0.4 through 5.0.5, FortiSandbox PaaS 5.0.4 through 5.0.5 may allow an unauthenticated attacker to execute unauthorized commands via specifically crafted HTTP requests	9.8	More Details
CVE-2026-36576	An OS command injection vulnerability in the app.py component of openlabs docker-wkhtmltopdf-aas up to commit 9f50579 allows attackers to execute arbitrary commands via a crafted POST request.	9.8	More Details
CVE-2017-20251	WordPress Insert PHP plugin versions before 3.3.1 contain a PHP code injection vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by injecting malicious shortcodes through the WordPress REST API. Attackers can send POST requests to the wp-json/wp/v2/posts endpoint with crafted content containing insert_php shortcodes to include and execute remote PHP files on the server.	9.8	More Details
CVE-2026-9698	DBI versions before 1.648 for Perl saved errors in a limited-sized buffer. Error messages that were returned when RaiseError, PrintError or HandleError were set were written to a 200-byte buffer without a length limit. Attackers that can influence the error text in an application can trigger a buffer overflow.	9.8	More Details
CVE-2026-5067	A remote, unauthenticated attacker can trigger memory corruption in Zephyr's HTTP server WebSocket upgrade path by sending a crafted Sec-WebSocket-Key header. The HTTP/1 header parser copies the header into a fixed-size buffer using a bounded copy that does not guarantee NUL termination when the input length reaches the buffer size. During upgrade handling the buffer is copied to a local stack buffer and passed to strlen(); if no NUL exists in-bounds, strlen() reads beyond the stack buffer and subsequent concatenation with the WebSocket magic string can write out of bounds. This leads to out-of-bounds read and write on stack memory, resulting in crash (denial of service) and potentially code execution. The path is reachable when CONFIG_HTTP_SERVER_WEBSOCKET is enabled.	9.8	More Details
CVE-2026-27671	Due to improper RFC protocol validation in the SAP Kernel used by the Application Server ABAP of SAP NetWeaver and ABAP Platform, an unauthenticated attacker can send a crafted RFC request that exploits logical errors in memory management, leading to memory corruption. This could lead to a high impact on the confidentiality, integrity, and availability of the application.	9.8	More Details
	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, an unsafe execution vulnerability exists		

CVE-2026-52778	in the Bazar form field calculator (CalcField.php) of YesWiki. The application attempts to sanitize user-defined mathematical formulas using a complex recursive regular expression before passing them to the PHP eval() function. This implementation is inherently flawed: it is vulnerable to Regular Expression Denial of Service (ReDoS / Stack Overflow) which can crash the server, and it creates a high-risk architecture where any logic bypass directly results in arbitrary PHP code execution. Version 4.6.6 patches the issue.	9.8	More Details
CVE-2026-39910	STACKIT IaaS API contains a missing authorization check vulnerability that allows authenticated, low-privileged attackers to escalate privileges to full organization compromise by attaching arbitrary service accounts to virtual machines they control. Attackers can exploit the unvalidated PUT servers service-accounts endpoint to attach high-privileged service accounts and query the Instance Metadata Service to retrieve OAuth2 tokens, bypassing tenant boundaries and gaining unauthorized control over the entire organization environment.	9.8	More Details
CVE-2026-25555	OpenBullet2 through version 0.3.2 contains an authentication bypass vulnerability in the API key authentication middleware that allows unauthenticated attackers to gain admin access by supplying an empty X-Api-Key header value. Attackers can exploit the middleware's comparison of the supplied header against an empty AdminApiKey default string to access the admin console and all API endpoints without valid credentials.	9.8	More Details
CVE-2026-44631	Buffer Underwrite vulnerability in Apache HTTP Server on crafted regular expressions in the configuration. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	9.8	More Details
CVE-2026-29167	Use After Free vulnerability in Apache HTTP Server with mod_ldap in per-directory configuration This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	9.8	More Details
CVE-2026-11499	A vulnerability was determined in Tenda HG7HG9 and HG10 300001138_en_xpon. This affects the function formDOMAINBLK of the file /boaform/formDOMAINBLK. Executing a manipulation of the argument blkDomain can lead to stack-based buffer overflow. The attack may be performed from remote.	9.8	More Details
CVE-2024-58348	WordPress Background Image Cropper version 1.2 contains a remote code execution vulnerability that allows unauthenticated attackers to upload arbitrary files by accessing the ups.php endpoint. Attackers can upload PHP files through the file upload form in the plugin directory to execute arbitrary code on the server.	9.8	More Details
CVE-2026-26142	Deserialization of untrusted data in Nuance PowerScribe allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2023-54352	WordPress Seotheme contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by uploading malicious files to the theme directory. Attackers can access the uploaded PHP shell at /wp-content/themes/seotheme/mar.php to execute system commands and upload additional files for persistent access.	9.8	More Details
CVE-2026-10580	The Hippoo Mobile App for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to and including 1.9.4. This is due to a logic conflation in HippooPermissions::get_user_permissions(), which returns the same null sentinel for both administrators and unauthenticated visitors — a value that HippooPermissions::has_role_access() unconditionally interprets as full administrator access — causing override_extension_permission_callback() to assign __return_true as the permission callback for every WordPress and WooCommerce REST route cloned under /wc-hippoo/v1/ext/ by HippooControllerWithAuth::re_register_external_routes(), while the block_unauthorized_access() pre-dispatch guard fails to block unauthenticated users for the same reason. This makes it possible for unauthenticated attackers to invoke any core REST endpoint without credentials — most critically, sending a POST request to /wc-hippoo/v1/ext/wp/v2/users/<id> with a {"password":"<new_password>"} body to reset the password of any WordPress user, including the site administrator, and gain full administrative control of the site.	9.8	More Details
CVE-2026-45748	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. The `POST /ssh/tunnel/connect` endpoint in Termix prior to version 2.3.2 builds an SSH tunnel command by interpolating user-controlled host record fields (`endpointIP`, `endpointUsername`, `password`) directly into a shell command without escaping, allowing persistent OS command injection on the source SSH host. Version 2.3.2 patches the issue.	9.8	More Details
CVE-2025-71318	NetMan 204 fails to enforce authentication on its administrative pages and command endpoints. A remote, unauthenticated attacker can directly request administrative pages (such as administration.html, administration-commands.html, and configuration.html) to disclose sensitive information including LDAP configuration and active user details, and can invoke privileged UPS	9.8	More Details

	control commands — including shutdown, reboot, switch-on-bypass, and battery test — without supplying any credentials.		
CVE-2025-71317	NetMan 204 contains a hard-coded backdoor account with the username and password 'eurek' that grants administrative access. A remote, unauthenticated attacker can authenticate through the cgi-bin/login.cgi endpoint (for example /cgi-bin/login.cgi?username=eurek&password=eurek, which due to lax parameter validation can be shortened to /cgi-bin/login.cgi?username=eurek%20eurek) to obtain administrator privileges, allowing them to alter device configuration, enable the telnet/SSH services, and reset local user credentials.	9.8	More Details
CVE-2026-11362	DataDog::DogStatsd versions through 0.07 for Perl allow metric injections from event tags. DataDog::DogStatsd does not properly sanitise input, allowing metric injections of data from untrusted sources. The format_event method (used by the event method) does not validate the content of the tags, which may contain commas (allowing tags to be injected) or newlines, pipes and colons that allow metric injections. (There is an ineffective s/|//g to remove pipes, but because the pipe is not escaped, it is interpreted as a regular expression metacharacter and has no effect.)	9.8	More Details
CVE-2026-10879	DBI versions before 1.648 for Perl have a heap overflow when preparsing SQL statements with more than 9 binders. The preparse method expands SQL placeholder characters to numbered binders of the form :pN, but only allocates three characters per binder in the buffer. Placeholders 10-99 require four characters, 100-999 require five characters, et cetera.	9.8	More Details
CVE-2026-6274	Improper Authentication, Missing authentication for critical function, Weak Authentication vulnerability in DTS Electronics Industry and Trade Ltd. Co. Redline WR3200 allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Redline WR3200: from 7.1.3 before 7.1.8.	9.8	More Details
CVE-2026-47065	ZDRES-232: resolveProxyClass Not Overridden - acceptMatchers Filter Bypass via java.lang.reflect.Proxy Assessment: Fully addressed. When the serialised stream contains a TC_PROXYCLASSDESC (the marker for a java.lang.reflect.Proxy), JDK's ObjectInputStream.readProxyDesc() is dispatched. JDK then calls the default ObjectInputStream.resolveProxyClass(interfaces) implementation, which performs Class.forName(intf, false, latestUserDefinedLoader()) for EACH interface name and constructs the proxy class â€" bypassing the accepted classes list . ZDRES-233: Class.forName(name, initialize=true, classLoader) in readClassDescriptor Triggers Static Initialiser of Allow-Listed Classes Assessment: Fully addressed. For ANY class on the allow-list, deserialising a stream that names it triggers the class's (static initialiser) BEFORE any instance is constructed. This means an attacker who supplies a class name on the allow-list (e.g., the developer wrote accept("com.myapp.*") , attacker supplies com.myapp.SomeClass) causes <clinit> of SomeClass â€" and many real-world classes have side-effecting static initialisers Both issues have been fixed.	9.8	More Details
CVE-2026-7763	A heap-based buffer overflow vulnerability in the morse.ko HaLow Wi-Fi kernel driver in Morse Micro HaLowLink 2 software versions prior to 2.11.13 allows an unauthenticated attacker within radio range to cause a Denial of Service (kernel panic) or potentially achieve Remote Code Execution via a crafted 802.11ah beacon frame containing a malformed Traffic Indication Map (TIM) Information Element. The function morse_page_slicing_process_tim_element() in page_slicing.c derives the TIM bitmap length directly from a received IE field without validating it against the fixed-size destination buffer before passing it to memset and memcpy operations, allowing up to 252 bytes of attacker-controlled data to be written beyond the buffer boundary. Because beacons are broadcast frames processed during passive scanning, no authentication, association, or user interaction is required.	9.8	More Details
CVE-2026-7762	A heap-based buffer overflow vulnerability in the dot11ah.ko HaLow Wi-Fi kernel driver in Morse Micro HaLowLink 2 software versions prior to 2.11.13 allows an unauthenticated attacker within radio range to cause a Denial of Service (kernel panic) or potentially achieve Remote Code Execution via a crafted 802.11ah beacon or probe response frame containing a malformed S1G Capabilities Information Element (IE element ID 0xD9). The function morse_dot11ah_find_s1g_caps_for_bssid() uses the IE length field directly as the size argument to memcpy without validating it against the 15-byte destination buffer. An attacker can supply up to 255 bytes, causing an overflow of up to 240 bytes of attacker-controlled data into adjacent kernel heap memory. The vulnerability is triggerable during normal scanning without authentication, association, or user interaction.	9.8	More Details
CVE-2026-49185	The FieldX MDM adb messaging topic passes unverified payloads directly into Runtime.exec(), allowing command/instruction injection.	9.8	More Details
CVE-2026-8025	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in MOSK Information Technologies Ltd. CBS Platform allows SQL Injection. This issue affects CBS Platform: through 09062026. NOTE: The vendor was contacted and it was learned that the product is not supported.	9.8	More Details
	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in		

CVE-2026-7486	Netcad Software Inc. E-İmar allows SQL Injection. This issue affects E-İmar: from 2.10.1.0 before 3.0.2.	9.8	More Details
CVE-2026-49841	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, the mod_verto HTTP request handler allocates a fixed 2 MiB buffer for a POST application/x-www-form-urlencoded body but accepts Content-Length up to just under 10 MiB. The body-read loop is bounded by Content-Length rather than the buffer size, producing an attacker-controlled heap overflow of up to ~8 MiB -- before the HTTP basic-auth check runs. This issue has been patched in version 1.11.1.	9.8	More Details
CVE-2025-67447	The network diagnosis (ping) module in Neterbit NW-431F Router 20241014-IR03 and before is vulnerable to OS command injection. The application does not properly sanitize user input in the IP address field before passing it to the system's ping command. An attacker can inject arbitrary OS commands, which will be executed with the privileges of the web server.	9.8	More Details
CVE-2025-67446	Improper Authentication (Authentication Bypass) exists in Neterbit NW-431F Router 20241014-IR03 and before. The router uses a weak/predictable cookie value for authentication. By modifying the cookie value (e.g., setting it to "admin"), an attacker can bypass the authentication schema and gain unauthorized access to admin functionalities.	9.8	More Details
CVE-2026-49186	The local MQTT broker does not enforce topic-level Access Control Lists (ACLs). This allows any client to subscribe using wildcard characters (# or +) to enumerate hidden network devices or publish rogue control commands.	9.8	More Details
CVE-2026-36182	GNCC GP5 v7.1.76 was discovered to utilize a weak hashing algorithm to protect the root password, possibly allowing attackers to obtain root credentials and privileges via a bruteforce attack.	9.8	More Details
CVE-2026-10045	Shenzhen Kangda Xin Intelligent Network Technology Company's router, model DR300, version 2.1.2.121, contains hardcoded login credentials and has telnet enabled by default on WAN and LAN interfaces. These vulnerabilities allow attackers to read and write to memory, modify firmware stored in flash, inspect active connections, and view currently connected devices.	9.8	More Details
CVE-2026-35905	T3 Technology CPE models T625Pro v1.0.07, T6825G v1.0.03, and T7281 v1.0.03 were discovered to contain a hardcoded password for root access under the "superadmin" account.	9.8	More Details
CVE-2026-35904	Incorrect access control in the web management interface of T3 Technology CPE models T625Pro v1.0.07, T6825G v1.0.03, and T7281 v1.0.03 allows unauthorized attackers to enable the Telnet service via sending a crafted request to a vulnerable CGI component.	9.8	More Details
CVE-2026-30141	An issue was discovered in bitbank2 AnimatedGIF v2.2.0. A buffer overflow in the DecodeLZW function allows remote attackers to cause a denial of service (crash) or potentially execute arbitrary code via a crafted GIF file.	9.8	More Details
CVE-2019-25741	Mobatek MobaXterm 12.1 contains a structured exception handling (SEH) based buffer overflow vulnerability in the username field of session files that allows remote attackers to execute arbitrary code. Attackers can craft a malicious MobaXterm sessions file with overflow data that triggers the vulnerability when imported and executed, enabling reverse shell execution with user privileges.	9.8	More Details
CVE-2019-25738	WordPress Hybrid Composer 1.4.6 contains an unauthenticated settings change vulnerability that allows unauthenticated attackers to modify WordPress options by exploiting the hc_ajax_save_option action. Attackers can send POST requests to the admin-ajax.php endpoint with the action parameter set to hc_ajax_save_option to enable user registration and set the default role to administrator, enabling account takeover.	9.8	More Details
CVE-2019-25729	PDF Signer 3.0 contains a server-side template injection vulnerability that allows unauthenticated attackers to execute arbitrary code by injecting PHP commands through the CSRF-TOKEN cookie parameter. Attackers can craft malicious cookie values containing template injection payloads like shell_exec() to execute system commands and retrieve sensitive information from the server.	9.8	More Details
CVE-2019-25727	WordPress Plugin ad manager wd 1.0.11 contains an arbitrary file download vulnerability that allows unauthenticated attackers to download sensitive files by manipulating the path parameter. Attackers can send GET requests to the edit.php endpoint with export=export_csv and a malicious path parameter to read arbitrary files like wp-config.php accessible to the web server.	9.8	More Details
CVE-2026-4104	Authorization bypass through User-Controlled SQL primary key vulnerability in Akmer Informatics Automation Industry and Trade Ltd. Co. TeknoPass allows SQL Injection. This issue affects TeknoPass: from 20210501 through 20260429.	9.8	More Details
CVE-2026-	The /v1/Plan service relies entirely on a shared global API token for full administrative management,	9.8	More

50214	allowing arbitrary creation of zero-cost network access plans.		Details
CVE-2026-50211	Leftover engineering diagnostics and factory-level diagnostic software remain exposed on retail builds, giving malicious apps write privileges to internal NVRAM registers.	9.8	More Details
CVE-2026-35075	An unauthenticated remote attacker can recover a default, hard coded password from a firmware image and thus gain full access to all affected devices.	9.8	More Details
CVE-2026-44815	Stack-based buffer overflow in Windows DHCP Client allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-49191	The production build of the M3WebServer hard-codes its backend API keys, which can be easily intercepted through verbose error handling pages.	9.8	More Details
CVE-2026-10880	OSNexus QuantaStor SDS Manager is vulnerable to SQL injection in the login endpoint. The username field is not properly sanitized before being incorporated into a SQL query, allowing an unauthenticated remote attacker to bypass authentication and log in as an administrator without supplying a valid password.	9.8	More Details
CVE-2026-47291	Integer overflow or wraparound in Windows HTTP.sys allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-47643	External control of file name or path in Azure Stack Edge allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-45447	Issue summary: A specially crafted PKCS#7 or S/MIME signed message could trigger a use-after-free during PKCS#7 signature verification. Impact summary: A use-after-free may result in process crashes, heap corruption, or potentially remote code execution. When processing a PKCS#7 or S/MIME signed message, if the SignedData digestAlgorithms field is present as an empty ASN.1 SET, OpenSSL may incorrectly free a caller-owned BIO during PKCS7_verify(). A subsequent use of the BIO by the calling application results in a use-after-free condition. In the common case this occurs when the application later calls BIO_free() on the BIO originally passed to PKCS7_verify(). Depending on allocator behavior and application-specific BIO usage patterns, this may result in a crash or other memory corruption. In some application contexts this may potentially be exploitable for remote code execution. Applications that process PKCS#7 or S/MIME signed messages using OpenSSL PKCS#7 APIs may be affected. Applications using the CMS APIs for this processing are not affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	9.8	More Details
CVE-2026-45657	Use after free in Windows Kernel allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-25550	Seagull Software BarTender 2010, 2016, and 2019 contain an unauthenticated remote code execution vulnerability in the .NET Remoting service exposed on TCP port 7375 via BtSystem.Service.exe. The service registers an unauthenticated singleton endpoint — BarTenderSystem for BarTender 2016 <= R9, and DataServiceSingleton for BarTender 2019 <= R10 — configured with BinaryServerFormatterSinkProvider and TypeFilterLevel set to Full. An unauthenticated remote attacker can exploit .NET Remoting object unmarshalling to read or write arbitrary files on the server using the .NET WebClient class, or coerce NTLMv2 authentication by supplying a UNC path to an attacker-controlled server, enabling sensitive credential disclosure, remote code execution, or lateral movement depending on service account privileges and network environment. The service runs in the context of NT AUTHORITY\SYSTEM.	9.8	More Details
CVE-2025-71316	SQLite 'sqldiff.exe' does not securely handle the way the Microsoft Windows C runtime converts Unicode characters to ANSI codepages. An attacker could use the '-L' option to load an arbitrary DLL with a crafted command line argument string that results in command line file arguments being misinterpreted as command line options. Fixed on or around 2025-12-26.	9.8	More Details
CVE-2026-5241	A vulnerability in the LightGlue model loading path of huggingface/transformers version 5.2.0 allows an attacker-controlled model repository to execute arbitrary code during model initialization. The issue arises because the `trust_remote_code` parameter, intended to prevent remote code execution, is overridden by untrusted serialized configuration data in a nested code path. Specifically, when loading a LightGlue model using `AutoModel.from_pretrained()` with `trust_remote_code=False`, the `LightGlueConfig` reads the `trust_remote_code` value from the untrusted `config.json` file and propagates it into nested `AutoConfig.from_pretrained()` calls. This results in the execution of attacker-provided Python modules, even when the victim explicitly disables remote code execution. The vulnerability poses a high risk for environments such as API inference servers, research notebooks, CI/CD pipelines, and model evaluation workers, potentially leading to credential theft, lateral movement, or persistence/backdoor deployment.	9.6	More Details
CVE-2026-	Use after free in Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to		More

11293	potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	Details
CVE-2026-11282	Insufficient policy enforcement in Sandbox in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-47928	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	9.6	More Details
CVE-2026-47281	Improper input validation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	9.6	More Details
CVE-2026-11697	Insufficient validation of untrusted input in UI in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-11671	Use after free in Navigation in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-11659	Integer overflow in UI in Google Chrome on Linux prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-11654	Use after free in CameraCapture in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-45758	Guardrails AI is a Python framework that helps build AI applications. On May 11, 2026 at approximately 6:00 PM Pacific, an attacker published a malicious version of `guardrails-ai` (0.10.1) to PyPI. Aany user who installed `guardrails-ai==0.10.1` from PyPI on May 11, 2026 may be affected. Security researchers identified the malicious package within approximately 2 hours of publication, and PyPI quarantined the repository. Based on our telemetry, Guardrails AI maintainers have observed no requests to Guardrails AI infrastructure originating from the malicious 0.10.1 version, and a review of system and access logs has produced no evidence of user data exfiltration through their systems. Users should upgrade to version 0.10.2 or downgrade to version 0.10.0, both of which are unaffected. Those who installed version 0.10.1 should rotate any credentials accessible from their machine (GitHub PATs, cloud provider keys, package registry tokens, API keys) and audit their GitHub account for unauthorized workflows or repositories.	9.6	More Details
CVE-2026-11651	Use after free in Network in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-11638	Use after free in Printing in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-11634	Use after free in Gamepad in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-42904	Heap-based buffer overflow in Windows TCP/IP allows an unauthorized attacker to elevate privileges over an adjacent network.	9.6	More Details
CVE-2026-11167	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11250	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2026-11070	Insufficient validation of untrusted input in Chromoting in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the network process to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11065	Use after free in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11063	Insufficient validation of untrusted input in WebNN in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details

CVE-2026-11213	Insufficient validation of untrusted input in Reading Mode in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11056	Insufficient validation of untrusted input in SiteIsolation in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11052	Type Confusion in GPU in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11047	Inappropriate implementation in Base in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11043	Out of bounds write in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11037	Out of bounds write in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11021	Insufficient validation of untrusted input in GPU in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11009	Use after free in USB in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11002	Use after free in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-10990	Use after free in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-10983	Insufficient validation of untrusted input in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-10974	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-10972	Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-10971	Insufficient validation of untrusted input in Printing in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-10966	Inappropriate implementation in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: High)	9.6	More Details
CVE-2026-10931	Use after free in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-10892	Out of bounds write in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-10886	Use after free in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-10881	Out of bounds read and write in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details

CVE-2024-27892	Affected platforms running Arista EOS with OpenConfig configured, a gNMI Set request can be run when it should have been rejected. This can result in unexpected configuration being applied to the switch.	9.6	More Details
CVE-2024-27890	Affected platforms running Arista EOS with OpenConfig configured, a gNMI Set request can be run when it should have been rejected. This can result in unexpected configuration being applied to the switch.	9.6	More Details
CVE-2026-35906	An undocumented debug CGI endpoint in T3 Technology CPE models T625Pro v1.0.07, T6825G v1.0.03 allows unauthenticated attackers to execute arbitrary system commands as root via supplying a crafted HTTP query string.	9.6	More Details
CVE-2026-8037	OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an un-authenticated attacker to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in multiple command endpoints	9.6	More Details
CVE-2026-11066	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11061	Type Confusion in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11114	Use after free in Device Trust in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11113	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11146	Insufficient validation of untrusted input in Chromoting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11131	Use after free in Autofill in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11163	Use after free in Messages in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11165	Use after free in WebMIDI in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11120	Insufficient validation of untrusted input in Enterprise Reporting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11119	Inappropriate implementation in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11198	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11207	Insufficient validation of untrusted input in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11152	Object lifecycle issue in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11112	Insufficient validation of untrusted input in Chromoting in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: Medium)	9.6	More Details

CVE-2026-11100	Use after free in File Input in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11095	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11094	Use after free in Codecs in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11088	Integer overflow in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-11082	Race in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-50208	High-risk TrustAllCerts routines disable standard TLS certificate validation. Combined with hard-coded DES symmetric encryption keys, a Man-in-the-Middle (MITM) actor could decrypt network traffic.	9.4	More Details
CVE-2026-41448	AdGuard Home, when started with the --glinet flag, contains an authentication bypass vulnerability that allows unauthenticated attackers to gain full admin access by supplying a path traversal sequence in the Admin-Token cookie, exploiting unsanitized string concatenation in the token file path construction within the authglinet middleware. Attackers can craft a request with a traversal payload in the Admin-Token header to redirect file reads to arbitrary paths.	9.4	More Details
CVE-2026-34691	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, potentially gaining elevated access or control over the victim's account or session. Scope is changed.	9.3	More Details
CVE-2026-50751	A logic flow weakness in Remote Access and Mobile Access certificate validation in deprecated IKEv1 key exchange allows an unauthenticated remote attacker to bypass user authentication and establish a remote access VPN connection without a valid user password.	9.3	More Details
CVE-2026-50225	The registration path /v1/account/register provides no bot mitigation mechanisms, allowing malicious automated systems to flood the database.	9.1	More Details
CVE-2026-45602	No cwe for this issue in Windows DHCP Server allows an unauthorized attacker to perform tampering over a network.	9.1	More Details
CVE-2026-50076	Deserialization of Untrusted Data in the Java replace-resolve path in Apache Fory fory-core Java SDK before 1.1.0 on Java/JVM platforms allows a remote attacker to bypass class registration, TypeChecker, and DisallowedList checks and invoke classpath-present readResolve/readExternal hooks via crafted Fory serialized data. Users are recommended to upgrade to version 1.1.0 or later, which fixes this issue.	9.1	More Details
CVE-2026-49840	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, esl_recv_event() parses Content-Length with atol() and passes the result straight to malloc(len + 1) with no sign or magnitude check. A malicious or man-in-the-middle ESL peer can send a frame with a negative Content-Length to corrupt the heap of, or crash, any process linked against libesl, before the client has authenticated to that peer. This issue has been patched in version 1.11.1.	9.1	More Details
CVE-2026-48040	The netty incubator codec.bhttp is a java language binary http parser. The library implements Oblivious HTTP (RFC 9458) using BoringSSL's HPKE C library via JNI. When deriving native memory addresses for cryptographic operations versions prior to 0.0.22.Final provide a fallback path for direct ByteBufs that do not expose their memory address through `hasMemoryAddress()`. This fallback occurs when `sun.misc.Unsafe` is unavailable to Netty — for example, when the JVM is started with `-Dio.netty.noUnsafe=true`, when a SecurityManager restricts Unsafe access, or when running on non-HotSpot JVMs. In these configurations, Netty's default `PooledByteBufAllocator` returns `PooledDirectByteBuf` instances for which `hasMemoryAddress()` returns false. Under the enabling JVM configuration, an unauthenticated network attacker can cause the OHTTP gateway to corrupt memory belonging to other concurrent connections and disclose the contents of adjacent pooled direct buffers by triggering cryptographic operations with crafted OHTTP requests. The corruption occurs regardless of whether the AEAD tag verification succeeds, as BoringSSL zeroizes the output buffer on failure. The information disclosure path provides the attacker with the encryption key	9.1	More Details

	needed to extract the leaked data. This violates the confidentiality and integrity of all connections sharing the same Netty buffer arena. Version 0.0.22.Final fixes the issue.		
CVE-2026-11153	Side-channel information leakage in Forms in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	9.1	More Details
CVE-2026-48579	Improper authorization in Microsoft Exchange Online allows an unauthorized attacker to disclose information over a network.	9.1	More Details
CVE-2026-9270	DataDog::DogStatsd versions through 0.07 for Perl allow metric injections. DataDog::DogStatsd does not properly sanitise input, allowing metric injections of data from untrusted sources. The send_stats method does not remove newlines from metric names ($stat variable), allowing attackers to change the metric name prefix. The send_stats method does not validate the content of the value ($delta variable), allowing attackers to inject metrics, especially from methods that do not restrict the data type for the value, such as set, gauge, count and histogram. The send_stats method does not validate the content of the tags, which may contain newlines, pipes and colons that allow metric injections. Note that the SYNOPSIS shows an example of passing a website form "loginName" parameter as a tag, which is unsafe.	9.1	More Details
CVE-2026-36500	An issue in the cluster-admin:backup-datastore component of Controller v12.0.5 allows attackers to execute a directory traversal via a crafted request.	9.1	More Details
CVE-2026-46266	In the Linux kernel, the following vulnerability has been resolved: inet: RAW sockets using IPPROTO_RAW MUST drop incoming ICMP Yizhou Zhao reported that simply having one RAW socket on protocol IPPROTO_RAW (255) was dangerous. socket(AF_INET, SOCK_RAW, 255); A malicious incoming ICMP packet can set the protocol field to 255 and match this socket, leading to FNHE cache changes. inner = IP(src="192.168.2.1", dst="8.8.8.8", proto=255)/Raw("TEST") pkt = IP(src="192.168.1.1", dst="192.168.2.1")/ICMP(type=3, code=4, nexthopmtu=576)/inner "man 7 raw" states: A protocol of IPPROTO_RAW implies enabled IP_HDRINCL and is able to send any IP protocol that is specified in the passed header. Receiving of all IP protocols via IPPROTO_RAW is not possible using raw sockets. Make sure we drop these malicious packets.	9.1	More Details
CVE-2025-10263	Arm C1-Ultra, C1-Premium, Neoverse V3 & V3AE, Neoverse V2, Neoverse V1, Neoverse-N2, Neoverse-N1, Cortex-X925, Cortex-X4, Cortex-X3, Cortex-X2, Cortex-X1 & X1C, Cortex-A710, Cortex-A78, A78AE & A78C, Cortex-A77, Cortex-A76 & A76A may allow writes to resources owned by a higher exception level.	9.1	More Details
CVE-2009-10007	Catalyst::Plugin::Authentication versions before 0.10_027 for Perl is susceptible to session fixation attacks. Catalyst::Plugin::Authentication does not automatically change the session id after authentication. An attacker that obtains a session id cookie can use this to impersonate the victim.	9.1	More Details
CVE-2026-46244	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_inner: Fix IPv6 inner_thoff desync In nft_inner_parse_l2l3(), when processing inner IPv6 packets, ipv6_find_hdr() correctly computes the transport header offset traversing all extension headers, but the result is immediately overwritten with nhoff + sizeof(_ip6h) (40 bytes), which only accounts for the IPv6 base header. This creates a desync between inner_thoff (wrong — points to extension header start) and l4proto (correct — e.g., IPPROTO_TCP), enabling transport header forgery and potential firewall bypass. This issue affects stable versions from Linux 6.2. For comparison, the normal (non-inner) IPv6 path correctly preserves ipv6_find_hdr()'s result. Removing the incorrect overwrite ensures that ipv6_find_hdr()'s calculated transport header offset is preserved, thereby fixing the desynchronization.	9.1	More Details
CVE-2026-42535	A path handling issue in mod_dav_fs in Apache 2.4.67 and earlier allows a WebDAV content author to directly manipulate trusted DAV property databases, potentially causing child process crashes. Users are recommended to upgrade to version 2.4.68, which fixes this issue.	9.1	More Details
CVE-2026-11393	Improper neutralization of triple-quote characters during Python code generation in AgentCore CLI before v0.14.2 might allow an authenticated remote threat actor to execute arbitrary code on AWS AgentCore Runtime under the imported agent's IAM execution role and on the local environment of another user in the same AWS account, via a crafted collaborationInstruction stored on a Bedrock Agent collaborator and later processed by that other user during agent import. To remediate this issue, users should upgrade to version 0.14.2.	9.0	More Details
CVE-2026-45750	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the GET /ssh/file_manager/ssh/resolvePath endpoint in the Termix File Manager component unsafely processes the path parameter and embeds it into a shell command executed over the active SSH session. Because the user-controlled value is placed inside double quotes and only double quotes are escaped, shell command substitution syntax such as $(...) is still interpreted by the remote shell. Version 2.3.2 fixes the issue.	9.0	More Details

CVE-2026-36748	RockRMS v16.13 and before v.17.7.0 is vulnerable to Cross Site Scripting (XSS) via Social Media links in user profile.	9.0	More Details
CVE-2026-40128	SAP NetWeaver Application Server Java (Web Container) allows an unauthenticated attacker to craft a malicious HTTP logon request that manipulates file inclusion parameters, enabling path traversal and processing of the included file. Processing the included file could allow the attacker to view or modify sensitive information or render any part of the local system unavailable.	9.0	More Details
CVE-2026-45746	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the File Manager functionality in Termix contains a critical Broken Access Control vulnerability due to improper validation of the sessionId parameter. The backend trusts a client-controlled identifier without verifying that it belongs to the authenticated user. This allows an attacker to manipulate the value and access active File Manager sessions belonging to other users. Since these sessions are tied to SSH connections to remote VPS instances, exploitation allows unauthorized interaction with another user's remote filesystem. Because the File Manager exposes functionality such as file reading, writing, uploading, and execution, this vulnerability enables direct command execution on another user's VPS (RCE). Version 2.3.2 patches the issue.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-43984	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 expose `log_js_errors` to any authenticated user, including guest users when guest access is enabled. The endpoint writes attacker-controlled strings directly into the main application log. The administrator-only `logFile` view then reads that log file and embeds it into an HTML response without escaping. This creates a stored cross-site scripting condition where a low-privilege guest can inject HTML or JavaScript into the log file and have it execute in an administrator's browser when the log viewer is opened. Version 2.17.1 patches the issue.	8.9	More Details
CVE-2026-10958	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10963	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 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-2026-10988	Use after free in Views in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10987	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 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-2026-10986	Integer overflow in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a malicious file. (Chromium security severity: High)	8.8	More Details
CVE-2026-10982	Use after free in WebXR in Google Chrome prior to 149.0.7827.53 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-2026-10978	Use after free in Chromoting in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: High)	8.8	More Details
CVE-2026-10975	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 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-2026-10965	Integer overflow in DevTools in Google Chrome prior to 149.0.7827.53 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-2026-10964	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 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-2026-10962	Type Confusion in Media in Google Chrome prior to 149.0.7827.53 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-2026-10991	Use after free in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-10959	Use after free in Input in Google Chrome on Android prior to 149.0.7827.53 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-2026-10957	Use after free in Glic in Google Chrome prior to 149.0.7827.53 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-2026-10956	Use after free in MimeHandlerView in Google Chrome prior to 149.0.7827.53 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-2026-10955	Type Confusion in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 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-2026-10954	Use after free in Actor in Google Chrome prior to 149.0.7827.53 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-2026-10952	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10951	Use after free in Autofill in Google Chrome on iOS prior to 149.0.7827.53 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: High)	8.8	More Details
CVE-2026-10989	Inappropriate implementation in V8 in Google Chrome prior to 149.0.7827.53 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: High)	8.8	More Details
CVE-2026-11557	A weakness has been identified in Tenda F451 1.0.0.7/1.0.0.9. The affected element is the function fromNatlimit of the file /goform/Natlimit of the component Web Management Interface. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-10948	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 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-2026-10995	Heap buffer overflow in TabStrip in Google Chrome prior to 149.0.7827.53 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-2026-11054	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11050	Use after free in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11049	Use after free in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11046	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11042	Use after free in Views in Google Chrome prior to 149.0.7827.53 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-2026-11041	Insufficient validation of untrusted input in Media in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11637	Use after free in Views in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-11633	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a malicious peripheral. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-11030	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11028	Use after free in Media in Google Chrome on Linux and ChromeOS prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11630	Use after free in File Input in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-11024	Stack buffer overflow in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11629	Use after free in Ozone in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-45484	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-11003	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11000	Use after free in Fonts in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-46490	samlify is a Node.js library for SAML single sign-on. Prior to version 2.13.0, samlify’s template substitution only escapes attribute contexts. Values inserted into element text (e.g., <saml:AttributeValue>) are not escaped. A normal user can inject XML markup into an attribute value (e.g., email, name) and add new <saml:Attribute> elements inside the signed assertion. The IdP then signs the tampered assertion and the SP accepts the injected attributes as trusted. This allows privilege escalation when attributes are used for authorization (roles/groups). This issue has been patched in version 2.13.0.	8.8	More Details
CVE-2026-11556	A security flaw has been discovered in Tenda F451 1.0.0.7/1.0.0.9. Impacted is the function formWriteFacMac of the file /goform/WriteFacMac of the component Web Management Interface. Performing a manipulation of the argument mac results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-10947	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 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-2026-11498	A vulnerability was found in Tenda HG7HG9 and HG10 300001138_en_xpon. Affected by this issue is the function asp_voip_OtherSet of the file /boaform/voip_other_set of the component Web Management Interface. Performing a manipulation of the argument funckey_transfer results in stack-based buffer overflow. The attack is possible to be carried out remotely.	8.8	More Details
CVE-2026-10897	Inappropriate implementation in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-			

2026-10895	Use after free in Ozone in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10893	Use after free in Chromoting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10891	Use after free in GFX in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10890	Use after free in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10888	Use after free in Cast Streaming in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10885	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10883	Type Confusion in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10882	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-45504	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-41236	Froxlor is open source server administration software. Version 2.3.6 contains a symlink-following flaw in the root-owned SSH key synchronization path used for customer FTP users. The provisioning code appends public keys to `~/.ssh/authorized_keys` under a customer-controlled home directory without verifying that the target path is not a symbolic link. If an attacker controls a shell-enabled customer account and can modify files inside the assigned home directory, the attacker can replace `~/.ssh/authorized_keys` with a symlink to `/root/.ssh/authorized_keys`. When Froxlor's privileged cron task later synchronizes SSH keys, it appends the attacker-supplied key into root's authorized key file, resulting in root SSH access. Version 2.3.7 contains a patch.	8.8	More Details
CVE-2026-5228	Improper Access Control, Missing Authorization vulnerability in Kurt Software Studio WriteUp Mobile App allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WriteUp Mobile App: from 1.3.0 through 04062026.	8.8	More Details
CVE-2026-43985	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 expose `configUpdate` as a state-changing administrator endpoint, but the route does not enforce `POST` and does not use any anti-CSRF token. In the default form and JWT-based authentication mode, the administrator session cookie is issued with `SameSite=Lax`, which still permits top-level cross-site navigation requests. An attacker can exploit this by luring a logged-in administrator to a malicious page that submits a cross-site request to `/configUpdate` and overwrites the local administrator username and password. The attacker can then sign in directly with the chosen credentials and take over the Tautulli administrative interface. Version 2.17.1 patches the issue.	8.8	More Details
CVE-2026-45648	Stack-based buffer overflow in Active Directory Domain Services allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2026-25855	OpenBullet2 through version 0.3.2 contains a remote code execution vulnerability that allows authenticated users to execute arbitrary commands by uploading script files (.bat.ps1.sh) through the FileProxySource proxy loading feature. Attackers can upload malicious script files as proxy sources, causing the server to execute the scripts and return output as proxy lines, resulting in arbitrary command execution on the host as the process user.	8.8	More Details
CVE-2026-47289	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	8.8	More Details

CVE-2026-47653	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-25559	OpenBullet2 through version 0.3.2 contains a path traversal vulnerability in the wordlist endpoint that allows authenticated attackers to perform arbitrary file read, write, and delete operations by supplying unsanitized absolute paths to the upload handler and wordlist functions. Attackers can chain the file write and delete primitives to achieve remote code execution by manipulating critical system files such as /etc/passwd, with full system impact since the application runs as root by default.	8.8	More Details
CVE-2026-10896	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10902	Use after free in Ozone in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-10945	Use after free in PDF in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-10903	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 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-2026-11553	A vulnerability was found in Tenda HG7HG9 and HG10 300001138_en_xpon. This affects the function formPPPEdit of the file /boaform/formPPPEdit. The manipulation of the argument encodename results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-10943	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 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-2026-10941	Out of bounds memory access in Skia in Google Chrome prior to 149.0.7827.53 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-2026-10939	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 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-2026-10936	Type Confusion in V8 in Google Chrome prior to 149.0.7827.53 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-2026-10935	Type Confusion in V8 in Google Chrome prior to 149.0.7827.53 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-2026-10932	Use after free in UI in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10928	Script injection in Headless in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10926	Use after free in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to execute arbitrary code via malicious network traffic. (Chromium security severity: High)	8.8	More Details
CVE-2026-10923	Use after free in WebAppInstalls in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to execute arbitrary code via a malicious file. (Chromium security severity: High)	8.8	More Details
CVE-2026-10922	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass same origin policy via malicious network traffic. (Chromium security severity: High)	8.8	More Details

CVE-2026-10914	Use after free in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 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-2026-10913	Use after free in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 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-2026-25856	OpenBullet2 through version 0.3.2 contains an authenticated remote code execution vulnerability that allows authenticated users to execute arbitrary C# code on the server host by creating or modifying job configurations. Attackers can leverage the plain C# execution mode, which lacks reference filtering or API restrictions, to access the file system, spawn processes, and invoke arbitrary .NET APIs as the process user.	8.8	More Details
CVE-2026-10910	Type Confusion in V8 in Google Chrome prior to 149.0.7827.53 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-2026-10907	Out of bounds write in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-10904	Inappropriate implementation in V8 in Google Chrome prior to 149.0.7827.53 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-2026-11055	Use after free in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11059	Use after free in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11060	Use after free in Media in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11262	Use after free in TabStrip in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-42985	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-5411	The WP Captcha PRO (the premium version of the Advanced Google reCAPTCHA plugin, both have the same slug) plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 5.38. This is due to a capability check in the save_ajax() function of the licensing module, combined with unrestricted file extraction in sync_cloud_protection(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files including PHP webshells to the server by injecting a malicious cloud_protection_url into the license meta, which the plugin then downloads and extracts without file type validation into a web-accessible uploads directory. This can be used for remote code execution. Note: The vulnerability can only be exploited with a remote URL if "allow_url_fopen" is enabled in the php.ini config.	8.8	More Details
CVE-2026-5415	The WP Captcha PRO (the premium version of the Advanced Google reCAPTCHA plugin, both have the same slug) plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 5.38. This is due to the ajax_run_tool() AJAX handler relying solely on a nonce check (check_ajax_referer) for security without performing any capability check, combined with the create_temporary_link tool allowing the generation of passwordless login links for arbitrary users, and the handle_temporary_links() function authenticating visitors via these links without any additional authorization validation. The required nonce is exposed to all authenticated backend users (including Subscribers) via wp_localize_script() on all non-settings admin pages when the plugin's welcome pointer has not been dismissed. This makes it possible for authenticated attackers, with Subscriber-level access and above, to bypass normal authentication and log in as any user, including Administrators, resulting in complete account takeover.	8.8	More Details
CVE-2026-11235	Insufficient policy enforcement in Compositing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details

CVE-2026-11230	Use after free in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11211	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11699	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11698	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11202	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11201	Use after free in ServiceWorker in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11191	Out of bounds memory access in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11188	Use after free in USB in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11688	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.103 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-2026-11687	Use after free in Dawn in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11683	Use after free in WebCodecs in Google Chrome prior to 149.0.7827.103 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-2026-11179	Inappropriate implementation in ORB in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11177	Use after free in Omnibox in Google Chrome prior to 149.0.7827.53 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-2026-11248	Inappropriate implementation in Google Lens in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11272	Insufficient validation of untrusted input in Reading List in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11175	Incorrect security UI in Messages in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-50733	Markdown Preview Enhanced before 0.8.28 parses WaveDrom diagrams by evaluating untrusted markdown content with eval(), allowing arbitrary JavaScript execution. The flaw affects every render path - the live preview (window.eval) and presentation mode plus HTML export (the bundled WaveDrom.ProcessAll()/eva() helpers) - and can also be triggered through a <script type="WaveDrom"> element injected via raw HTML in markdown. When a victim previews or exports a crafted markdown document, an attacker can execute arbitrary code, leading to arbitrary file write. Fixed in 0.8.28 by	8.8	More Details

	parsing with JSON5.parse() and sanitizing WaveDrom data scripts to inert strict JSON.		
CVE-2026-11616	The Events Calendar for GeoDirectory plugin for WordPress is vulnerable to Privilege Escalation in versions up to and including 2.3.28. This is due to the ajax_ayi_action() handler only applying strip_tags(esc_sql()) — with no allow-list — to the attacker-controlled $_POST['type'] and $_POST['postid'] values before forwarding them to update_ayi_data(), which calls update_user_meta($current_user->ID, $rsvp_args['type'], $posts). By passing type=wp_capabilities and postid=administrator, an attacker writes ['subscriber'=>true,'administrator'=>'administrator'] into their own wp_capabilities user meta; WP_User::get_role_caps() then treats the 'administrator' array key as an active role on the next request. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to Administrator.	8.8	More Details
CVE-2026-11572	Versions of the package degit before 2.8.6, from 3.0.0 and before 3.3.1 are vulnerable to Command Injection due to improper sanitisation of user input for git shell commands directly invoked with exec() method by _cloneWithGit() and fetchRefs() functions. An attacker can execute arbitrary operating system commands as the process user by supplying a specially crafted git repository name.	8.8	More Details
CVE-2026-8365	The Blocksy theme for WordPress is vulnerable to PHP Object Injection leading to Remote Code Execution via the 'blocksy_meta' REST API field and the V200 database migration in versions up to and including 2.1.35. This is due to insufficient input sanitization in the blocksy_sanitize_post_meta_options() function, which only blocks values containing '<' or '>' and does not prevent serialized PHP object strings from being stored in post meta, combined with the SearchReplacer::run_recursively() function unconditionally deserializing all string values via @unserialize() during migration without restricting allowed classes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a serialized Blocksy\RaiiPattern object into post meta that, when the V200 migration runs on an upgraded site, is deserialized and triggers RaiiPattern::__destruct(), which executes arbitrary PHP callables via call_user_func().	8.8	More Details
CVE-2026-46746	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The application does not properly sanitize user input in the /api/sftp/uploadFiles endpoint, allowing the injection of shell command payloads via crafted directory names. These payloads are stored and executed when directory listings are retrieved. This could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system with the privileges of the affected service user (sinecins).	8.8	More Details
CVE-2026-46748	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected system includes a binary that is configured with the cap_dac_override capability. This capability allows the process to bypass file system permission checks, resulting in unrestricted file system access. This could allow a local attacker to escalate privileges leading to arbitrary file modification and gaining root privileges on the system.	8.8	More Details
CVE-2026-32193	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Azure Kubernetes Service allows an authorized attacker to execute code locally.	8.8	More Details
CVE-2026-40371	Improper handling of insufficient permissions or privileges in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-11307	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11306	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11305	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11304	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11303	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-11301	Inappropriate implementation in LiveCaption in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via malicious network traffic. (Chromium security severity: Low)	8.8	More Details

CVE-2026-11295	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-49492	Markdown Preview Enhanced before 0.8.28 opens external files and links from the preview through a shell and does not validate untrusted inputs taken from the markdown document - the diagram filename attribute, imported file paths, and the latex_engine code-chunk attribute. On Windows, a crafted markdown document can inject operating system commands that execute when the document is previewed. Fixed in 0.8.28 by passing these inputs as literal arguments instead of through a shell and validating them before use.	8.8	More Details
CVE-2026-49493	Markdown Preview Enhanced before 0.8.28 parses Bitfield fenced code blocks with interpretJS(), which evaluates the block content as code via vm.runInNewContext(), allowing arbitrary code execution. A crafted markdown document containing a malicious bitfield code block executes attacker-controlled code on the server side when the document is rendered or exported. Fixed in 0.8.28 by parsing bitfield register definitions with JSON5.parse(), since they are purely data.	8.8	More Details
CVE-2026-11279	Out of bounds read in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-7654	The Admin Columns plugin for WordPress is vulnerable to PHP Object Injection leading to Remote Code Execution in versions up to and including 7.0.18. This is due to the use of `unserialize()` without an `allowed_classes` restriction in the `IdsToCollection::get_ids_from_string()` function, which processes attacker-controlled post meta values without proper validation. This makes it possible for authenticated attackers with Contributor-level access and above to inject a serialized PHP object into a post's custom meta field and trigger arbitrary code execution by exploiting a bundled POP gadget chain, resulting in remote code execution as the web server user.	8.8	More Details
CVE-2026-11173	Out of bounds write in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11413	A security vulnerability has been detected in JingDong JD Cloud Box AX6600 4.5.3.r4546. The impacted element is the function set_macfilter of the file /sbin/jdcweb_rpc. The manipulation leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-11657	Use after free in Payments in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11650	Use after free in V8 in Google Chrome prior to 149.0.7827.103 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-2026-11649	Use after free in V8 in Google Chrome prior to 149.0.7827.103 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-2026-11092	Insufficient policy enforcement in DevTools in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11091	Inappropriate implementation in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11648	Use after free in FullScreen in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11517	A vulnerability was determined in UTT HiPER 2610G up to 3.0.0-171107. This impacts the function strcpy of the file /goform/formConfigDnsFilterGlobal. Executing a manipulation of the argument GroupName can lead to buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-11086	Inappropriate implementation in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details

CVE-2026-11085	Integer overflow in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11646	Use after free in ViewTransitions in Google Chrome prior to 149.0.7827.103 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-2026-11080	Use after free in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11079	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory write via a crafted video file. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11077	Bad cast in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11076	Type Confusion in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11645	Out of bounds read and write in V8 in Google Chrome prior to 149.0.7827.103 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-2026-11074	Use after free in WebRTC in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11071	Use after free in Base in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11068	Use after free in WebSockets in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11102	Inappropriate implementation in Isolated Web Apps in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a malicious file. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11108	Inappropriate implementation in NFC in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11172	Incorrect security UI in Contact Picker in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11116	Use after free in Chromoting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11171	Integer overflow in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11164	Use after free in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11681	Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11680	Use after free in Media in Google Chrome on Windows prior to 149.0.7827.103 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-2026-11147	Use after free in WebML in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11144	Use after free in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted video file. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11674	Use after free in Guest View in Google Chrome prior to 149.0.7827.103 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-2026-11673	Use after free in InterestGroups in Google Chrome prior to 149.0.7827.103 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-2026-11670	Use after free in PDF in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	8.8	More Details
CVE-2026-11136	Use after free in Canvas in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11664	Use after free in Payments in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-11130	Use after free in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11662	Type Confusion in Bindings in Google Chrome prior to 149.0.7827.103 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-2026-11125	Use after free in Compositing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11124	Integer overflow in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11118	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-11117	Use after free in Views in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-49959	Hermes WebUI before version 0.51.311 contains a remote code execution vulnerability that allows authenticated attackers to execute arbitrary commands by placing malicious executable Git configuration in a workspace repository's .git/config file. Attackers can exploit Git subprocess invocations in api/workspace_git.py through vectors such as core.fsmonitor during git status, protocol.ext.allow with ext:: remotes during git fetch, credential.helper, core.askPass, core.gitProxy, or inherited environment variables including GIT_SSH_COMMAND to achieve arbitrary command execution on the host running the application.	8.8	More Details
CVE-2026-48095	7-Zip is a file archiver with a high compression ratio. Versions 26.00 and prior contain a heap buffer overflow vulnerability caused by an under-allocation in the NTFS compressed stream buffer (GetCuSize shift UB), potentially allowing attackers to cause arbitrary code execution or application crashes. CInStream::GetCuSize() in the NTFS handler computes the compression-unit buffer size as (UInt32)1 << (BlockSizeLog + CompressionUnit), and a crafted image with ClusterSizeLog >= 28 and CompressionUnit == 4 drives the exponent to 32, which is undefined behavior and collapses on x86/x64 so _inBuf is allocated as 1 byte. ReadStream_FALSE then writes up to 256 MB of attacker-controlled data into that 1-byte buffer in 64 KB iterations, and because the CInStream object sits only 304 bytes after _inBuf, its vtable pointer is overwritten and the next dispatched call achieves a vtable hijack. On 32-bit builds the overflow is unconditionally reached; on 64-bit it requires the parallel 8 GB _outBuf allocation to succeed,	8.8	More Details

	otherwise failing closed to denial of service. The NTFS handler is enabled by default in stock 7z.dll and, via signature-based fallback matching "NTFS " at offset 3, will open a crafted image regardless of file extension during extraction or testing. Version 26.01 fixes the issue.		
CVE-2026-35083	A remote attacker with user privileges can exploit a stack buffer overflow to gain full system access as root.	8.8	More Details
CVE-2026-36607	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 allows unauthenticated brute-force attacks via the TDDP password change endpoint (code=10), which lacks the rate limiting applied to the login endpoint (code=7). An attacker on the adjacent network can attempt unlimited passwords without triggering account lockout.	8.8	More Details
CVE-2026-35082	The ugw-logread method allows a remote attacker with user privileges to access arbitrary local files due to insufficient validation of user-supplied input.	8.8	More Details
CVE-2026-49190	The system fails to evaluate instructional permissions over multiple internal operation codes (opcodes), permitting unauthorized application installations or command executions.	8.8	More Details
CVE-2026-11528	A vulnerability was found in Tenda AC18 15.03.05.05. The affected element is the function sub_45304 of the file /goform/getRebootStatus of the component Web Management Interface. The manipulation of the argument callback results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-46480	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, evaluator create and update mass-assignment allows cross-workspace evaluator takeover. This issue has been patched in version 3.1.2.	8.8	More Details
CVE-2026-46656	Bludit is a content management system. Versions prior to 3.22.0 have a Broken Access Control flaw where active sessions remain valid even after the corresponding user account has been physically deleted from the database. This "Ghost Session" allows revoked users to maintain full unauthorized access to the system. Version 3.22.0 fixes the issue.	8.8	More Details
CVE-2026-35084	A remote attacker with user privileges can exploit a stack buffer overflow in dali-devconfig to gain full system access as root.	8.8	More Details
CVE-2026-49194	The debugging routine SCREEN_CLICK(5053) enables a connection to skip the standard device login prompt entirely and directly enter an interactive shell interface.	8.8	More Details
CVE-2026-11504	A vulnerability was detected in Tenda CX12L 16.03.53.12. The impacted element is the function setSchedWifi of the file /goform/openSchedWifi of the component Wi-Fi Schedule Configuration Endpoint. Performing a manipulation of the argument schedStartTime/schedEndTime results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-35085	A remote attacker with user privileges can exploit a stack buffer overflow in gdv-serverconfig to gain full system access as root.	8.8	More Details
CVE-2026-11503	A security vulnerability has been detected in Tenda CX12L 16.03.53.12. The affected element is the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set of the component Wi-Fi Configuration Endpoint. Such manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-36608	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 allows UPnP AddPortMapping to forward external ports to the router's own admin interface by accepting its own IP (192.168.1.1) or localhost (127.0.0.1) as InternalClient. An unauthenticated LAN attacker can expose the admin panel to the internet with a single SOAP request.	8.8	More Details
CVE-2026-50636	The RemoteControl API methods invite_participants and remind_participants pass a caller-supplied token-ID array into TokenDynamic::findUninvited(), which concatenates the values directly into a tid IN ('...') SQL clause without parameterization or input validation. A remote, authenticated attacker holding the tokens/update permission on a survey can inject a crafted array element to perform SQL injection. Because LimeSurvey configures its PDO connection with emulated prepared statements (emulatePrepare = true) and does not disable MySQL multi-statements, the injection supports stacked queries: the attacker can append arbitrary additional statements (INSERT/UPDATE/DELETE/DROP/CREATE) after the original SELECT. This permits both arbitrary read of any data in the database, such as administrator bcrypt password hashes (lime_users), survey response PII, session records, and global settings, all	8.8	More Details

	recoverable via a SLEEP() time-based blind oracle, and arbitrary write/destruction of that data, including directly overwriting the administrator password hash for immediate account takeover or dropping/truncating tables. Reads and writes extend to any schema the application's database user can access. The RemoteControl interface (RPCInterface = json/xml) must be enabled, which is not the default.		
CVE-2026-50635	LimeSurvey constructs account password-reset links from the client-supplied HTTP Host header without validating it. The optional allowedHosts allowlist that would constrain this is undefined in the default (and documented) configuration, so LSHttpRequest::checkIsAllowedHost() results in no operation. A remote, unauthenticated attacker who submits a forgotten-password request for a known account (requiring only the target's username and email) with a spoofed Host header causes LimeSurvey to email that account a reset link whose hostname is attacker-controlled while embedding the genuine validation_key. When the recipient or an automated inbound mail-security link scanner dereferences the link, the valid reset token is disclosed to the attacker, who replays it against the legitimate host's newPassword endpoint to set a new password and take over the account.	8.8	More Details
CVE-2025-15656	Incorrect Privilege Assignment vulnerability in Mojoomla School Management allows Privilege Escalation. This issue affects School Management: from n/a through 93.2.0.	8.8	More Details
CVE-2026-41860	CWE-326 in BOSH allows a local attacker to steal Basic-auth credentials or redirect UAA token requests via MITM. HttpRequestHelper#create_async_endpoint and #send_http_get_request_synchronous hard-code OpenSSL::SSL::VERIFY_NONE, enabling an attacker to intercept traffic between bosh-monitor and the BOSH director or UAA and steal credentials. Affected versions: - BOSH: all versions prior to v282.1.9 (inclusive); fixed in v282.1.9 or later	8.8	More Details
CVE-2026-47932	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access unauthorized files or directories outside the intended restrictions. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	8.8	More Details
CVE-2025-14772	Authorization bypass through User-Controlled key vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	8.8	More Details
CVE-2026-11524	A vulnerability has been found in Tenda W20E 15.11.0.6. Impacted is the function modifyWifiFilterRules of the file /goform/modifyWifiFilterRules of the component Web Management Interface. The manipulation of the argument wifiFilterListRemark leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-11523	A flaw has been found in Tenda W20E 15.11.0.6. This issue affects the function formPortalAuth of the file /goform/PortalAuth of the component Web Management Interface. Executing a manipulation of the argument gotoUrl can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-11522	A vulnerability was detected in Tenda W20E 15.11.0.6. This vulnerability affects the function formSetPortMirror of the file /goform/setPortMirror. Performing a manipulation of the argument portMirrorMirroredPorts results in stack-based buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-46264	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pf: Fix sysfs initialization In case of devm_add_action_or_reset() failure the provided cleanup action will be run immediately on the not yet initialized kobject. This may lead to errors like: [ ] kobject: '(null)' (ff110001393608e0): is not initialized, yet kobject_put() is being called. [ ] WARNING: lib/kobject.c:734 at kobject_put+0xd9/0x250, CPU#0: kworker/0:0/9 [ ] RIP: 0010:kobject_put+0xdf/0x250 [ ] Call Trace: [ ] xe_sriov_pf_sysfs_init+0x21/0x100 [xe] [ ] xe_sriov_pf_init_late+0x87/0x2b0 [xe] [ ] xe_sriov_init_late+0x5f/0x2c0 [xe] [ ] xe_device_probe+0x5f2/0xc20 [xe] [ ] xe_pci_probe+0x396/0x610 [xe] [ ] local_pci_probe+0x47/0xb0 [ ] refcount_t: underflow; use-after-free. [ ] WARNING: lib/refcount.c:28 at refcount_warn_saturate+0x68/0xb0, CPU#0: kworker/0:0/9 [ ] RIP: 0010:refcount_warn_saturate+0x68/0xb0 [ ] Call Trace: [ ] kobject_put+0x174/0x250 [ ] xe_sriov_pf_sysfs_init+0x21/0x100 [xe] [ ] xe_sriov_pf_init_late+0x87/0x2b0 [xe] [ ] xe_sriov_init_late+0x5f/0x2c0 [xe] [ ] xe_device_probe+0x5f2/0xc20 [xe] [ ] xe_pci_probe+0x396/0x610 [xe] [ ] local_pci_probe+0x47/0xb0 Fix that by calling kobject_init() and kobject_add() separately and register cleanup action after the kobject is initialized. Also make this cleanup registration a part of the create helper to fix another mistake, as in the loop we were wrongly passing parent kobject while registering cleanup action, and this resulted in some undetected leaks. (cherry picked from commit 98b16727f07e26a5d4de84d88805ce7ffcfdd324)	8.8	More Details
	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0 of HAX CMS PHP, the `saveFile` endpoint validates upload extensions case-insensitively and writes the filename		

CVE-2026-46392	to disk verbatim, but the `.htaccess` rule that forces `Content-Disposition: attachment` on HTML files is case-sensitive. An HTML file uploaded with an uppercase extension (`.HTML`, `.Html`, `.HTM`) is still served as `text/html` but the forced-download header never applies, so the browser renders it inline and executes any embedded JavaScript in the HAXcms origin. This bypasses the mitigation shipped for CVE-2026-22704. Version 26.0.0 contains a fix.	8.7	More Details
CVE-2026-41031	A Stored Cross-Site Scripting vulnerability in Vinna Process Monitor Version 4.0 Service Pack 1 (Build 63255) allows an authenticated remote attacker with low privileges to inject malicious JavaScript code into the application. This enables attackers to steal administrative access tokens and session credentials.	8.7	More Details
CVE-2026-46273	In the Linux kernel, the following vulnerability has been resolved: ibmveth: Disable GSO for packets with small MSS Some physical adapters on Power systems do not support segmentation offload when the MSS is less than 224 bytes. Attempting to send such packets causes the adapter to freeze, stopping all traffic until manually reset. Implement ndo_features_check to disable GSO for packets with small MSS values. The network stack will perform software segmentation instead. The 224-byte minimum matches ibmvnic commit <f10b09ef687f> ("ibmvnic: Enforce stronger sanity checks on GSO packets") which uses the same physical adapters in SEA configurations. The issue occurs specifically when the hardware attempts to perform segmentation (gso_segs > 1) with a small MSS. Single-segment GSO packets (gso_segs == 1) do not trigger the problematic LSO code path and are transmitted normally without segmentation. Add an ndo_features_check callback to disable GSO when MSS < 224 bytes. Also call vlan_features_check() to ensure proper handling of VLAN packets, particularly QinQ (802.1ad) configurations where the hardware parser may not support certain offload features. Validated using iptables to force small MSS values. Without the fix, the adapter freezes. With the fix, packets are segmented in software and transmission succeeds. Comprehensive regression testing completedd (MSS tests, performance, stability).	8.6	More Details
CVE-2026-49202	Internal multimedia session archives are accessible without authentication, exacerbated by loose Cross-Origin Resource Sharing (CORS) rules that allow cross-site theft.	8.6	More Details
CVE-2026-11158	Insufficient validation of untrusted input in Downloads in Google Chrome on Mac prior to 149.0.7827.53 allowed a local attacker to potentially perform a sandbox escape via a crafted AppleScript command. (Chromium security severity: Medium)	8.6	More Details
CVE-2026-47906	Dreamweaver Desktop versions 21.7 and earlier are affected by a Dependency on Vulnerable Third-Party Component vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	8.6	More Details
CVE-2026-20230	A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device. This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to write files to the underlying operating system that could be used later to elevate to root. Note: Cisco has assigned this security advisory a Security Impact Rating (SIR) of Critical rather than High as the score indicates. The reason is that exploitation of this vulnerability could result in an attacker elevating privileges to root. Note: To exploit this vulnerability, the WebDialer service must be enabled. WebDialer is disabled by default.	8.6	More Details
CVE-2026-44810	Improper authentication in Windows Cryptographic Services allows an unauthorized attacker to elevate privileges locally.	8.4	More Details
CVE-2026-45463	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-45641	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-45456	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-45461	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Stack Edge	8.4	More

41098	allows an authorized attacker to perform spoofing over a network.		Details
CVE-2026-45607	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-47929	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could exploit this vulnerability to gain elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed.	8.4	More Details
CVE-2026-47931	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	8.4	More Details
CVE-2026-46270	In the Linux kernel, the following vulnerability has been resolved: power: supply: rt9455: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.	8.4	More Details
CVE-2026-45472	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-45474	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-26422	clash-verge-service-ipc before 2.3.0 has a world-reachable IPC endpoint, leading to local privilege escalation.	8.4	More Details
CVE-2026-46251	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix block_group_tree dirty_list corruption When the incompat flag EXTENT_TREE_V2 is set, we unconditionally add the block group tree to the switch_commits list before calling switch_commit_roots, as we do for the tree root and the chunk root. However, the block group tree uses normal root dirty tracking and in any transaction that does an allocation and dirties a block group, the block group root will already be linked to a list by the dirty_list field and this use of list_add_tail() is invalid and corrupts the prev/next members of block_group_root->dirty_list. This is apparent on a subsequent list_del on the prev if we enable CONFIG_DEBUG_LIST: [32.1571] ------------[cut here]------------ [32.1572] list_del corruption. next->prev should beffff958890202538, but was ffff9588992bd538. (next=ffff958890201538) [32.1575] WARNING: lib/list_debug.c:65 at 0x0, CPU#3: sync/607 [32.1583] CPU: 3 UID: 0 PID: 607 Comm: sync Not tainted 6.18.0 #24PREEMPT(none) [32.1585] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS1.17.0-4.fc41 04/01/2014 [32.1587] RIP: 0010:__list_del_entry_valid_or_report+0x108/0x120 [32.1593] RSP: 0018:ffffaa288287fdd0 EFLAGS: 00010202 [32.1594] RAX: 0000000000000001 RBX: ffff95889326e800 RCX:ffff958890201538 [32.1596] RDX: ffff9588992bd538 RSI: ffff958890202538 RDI:ffffffff82a41e00 [32.1597] RBP: ffff958890202538 R08: ffffffff828fc1e8 R09:00000000ffffefff [32.1599] R10: ffffffff8288c200 R11: ffffffff828e4200 R12:ffff958890201538 [32.1601] R13: ffff95889326e958 R14: ffff958895c24000 R15:ffff958890202538 [32.1603] FS: 00007f0c28eb5740(0000) GS:ffff958af2bd2000(0000)knlGS:0000000000000000 [32.1605] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [32.1607] CR2: 00007f0c28e8a3cc CR3: 0000000109942005 CR4:0000000000370ef0 [32.1609] Call Trace: [32.1610] <TASK> [32.1611] switch_commit_roots+0x82/0x1d0 [btrfs] [32.1615] btrfs_commit_transaction+0x968/0x1550 [btrfs] [32.1618] ? btrfs_attach_transaction_barrier+0x23/0x60 [btrfs] [32.1621] __iterate_supers+0xe8/0x190 [32.1622] ? __pfx_sync_fs_one_sb+0x10/0x10 [32.1623] ksys_sync+0x63/0xb0 [32.1624] __do_sys_sync+0xe/0x20 [32.1625] do_syscall_64+0x73/0x450 [32.1626] entry_SYSCALL_64_after_hwframe+0x76/0x7e [32.1627] RIP: 0033:0x7f0c28d05d2b [32.1632] RSP: 002b:00007ffc9d988048 EFLAGS: 00000246 ORIG_RAX:00000000000000a2 [32.1634] RAX: ffffffffffffffda RBX: 00007ffc9d988228 RCX:00007f0c28d05d2b [32.1636] RDX: 00007f0c28e02301 RSI: 00007ffc9d989b21 RDI:00007f0c28dba90d [32.1637] RBP: 0000000000000001 R08: 0000000000000001	8.4	More Details

	R09:0000000000000000 [32.1639] R10: 0000000000000000 R11: 0000000000000246 R12:000055b96572cb80 [32.1641] R13: 000055b96572b19f R14: 00007f0c28dfa434 R15:000055b96572b034 [32.1643] </TASK> [32.1644] irq event stamp: 0 [32.1644] hardirqs last enabled at (0): [<0000000000000000>] 0x0 [32.1646] hardirqs last disabled at (0): [<ffffffff81298817>]copy_process+0xb37/0x2260 [32.1648] softirqs last enabled at (0): [<ffffffff81298817>]copy_process+0xb37/0x2260 [32.1650] softirqs last disabled at (0): [<0000000000000000>] 0x0 [32.1652] ---[end trace 0000000000000000]--- Furthermore, this list corruption eventually (when we happen to add a new block group) results in getting the switch_commits and dirty_cowonly_roots lists mixed up and attempting to call update_root on the tree root which can't be found in the tree root, resulting in a transaction abort: [87.8269] BTRFS critical (device nvme1n1): unable to find root key (1 0 0) in tree 1 [87.8272] ------------[cut here]------------ [87.8274] BTRFS: Transaction aborted (error -117) [87.8275] WARNING: fs/btrfs/root-tree.c:153 at 0x0, CPU#4: sync/703 [87.8285] CPU: 4 UID: 0 PID: 703 Comm: sync Not tainted 6.18.0 #25 PREEMPT(none) [87.8287] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-4.fc41 0 ---truncated---		
CVE-2026-45482	Improper limitation of a pathname to a restricted directory ('path traversal') in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	8.4	More Details
CVE-2026-47635	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-45458	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2019-25735	AllPlayer 7.4 contains a local buffer overflow vulnerability in URL handling that allows attackers to overwrite structured exception handling pointers by supplying an excessively long URL string. Attackers can craft a malicious URL, paste it into the Open URL dialog, and trigger SEH-based code execution to run arbitrary commands with user privileges.	8.4	More Details
CVE-2019-25733	NetShareWatcher 1.5.8.0 contains a structured exception handler buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying malicious input. Attackers can craft a payload with overwritten SEH and NSEH pointers through the Restrictions custom filter field to trigger code execution when the Find function is invoked.	8.4	More Details
CVE-2019-25736	LabF nfsAxe 3.7 Ping Client contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious payload in the Host IP field. Attackers can craft a specially formatted input file with shellcode and overwrite the return address to execute calc.exe or other arbitrary commands.	8.4	More Details
CVE-2026-10970	Insufficient validation of untrusted input in InterestGroups in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10894	Use after free in Printing in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-10967	Use after free in SurfaceCapture in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10961	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10960	Uninitialized Use in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10898	Stack buffer overflow in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-10953	Use after free in Core in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details

CVE-2026-10949	Heap buffer overflow in Video in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10940	Race in Codecs in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-46481	OpenMetadata is a unified metadata platform. Prior to version 1.12.4, a non-admin SSO user can trigger a TEST_CONNECTION workflow for a Database Service and receive, in the HTTP 201 response of POST /api/v1/automations/workflows, both the cleartext database password in request.connection.config.password and the ingestion bot JWT in openMetadataServerConnection.securityConfig.jwtToken. The leaked ingestion-bot token can then be reused as Authorization: Bearer <jwt> to access sensitive service APIs with bot-level privileges. This issue has been patched in version 1.12.4.	8.3	More Details
CVE-2026-11256	Integer overflow in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	8.3	More Details
CVE-2026-10934	Use after free in Autofill in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10933	Use after free in Audio in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10929	Heap buffer overflow in ANGLE in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11236	Insufficient policy enforcement in Web Bluetooth in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	8.3	More Details
CVE-2026-10927	Out of bounds read in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10925	Out of bounds write in Skia in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10924	Integer overflow in Chromecast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10921	Integer overflow in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10920	Insufficient validation of untrusted input in WebShare in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10919	Use after free in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10918	Use after free in Viz in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10917	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10915	Use after free in Core in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details

CVE-2026-10911	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10909	Use after free in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11237	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	8.3	More Details
CVE-2026-11012	Use after free in Serial in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-11010	Use after free in WebShare in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-10905	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11679	Use after free in Codecs in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11677	Race in Network in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the network process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11676	Insufficient validation of untrusted input in Dawn in Google Chrome on Linux and ChromeOS prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11672	Heap buffer overflow in GPU in Google Chrome on Android prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11682	Inappropriate implementation in Views in Google Chrome on Linux prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11663	Use after free in Skia in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11661	Use after free in Views in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11660	Insufficient validation of untrusted input in New Tab Page in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11656	Use after free in ServiceWorker in Google Chrome prior to 149.0.7827.103 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: High)	8.3	More Details
CVE-2026-11655	Integer overflow in Media in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2025-5088	An authenticated Redis session could be used to obtain full root access to all servers in the CVX cluster. Note that this would require an attacker to have both network access to the Redis service on a CVX server and the Redis password. Please note that all Redis communication, including authentication, occurs over plaintext in the present day. TLS support is tracked under RFE1294850.	8.3	More Details
CVE-2026-	Use after free in Extensions in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.3	More Details

11652	(Chromium security severity: High)		
CVE-2026-11647	Use after free in Printing in Google Chrome on Android prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-10884	Use after free in Chromecast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-11642	Use after free in Web Apps in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-49203	Crucial management API endpoints for cellular eSIM allocation do not validate caller authorization, allowing remote profiles to be rewritten or deleted.	8.3	More Details
CVE-2026-11640	Integer overflow in libyuv in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-11040	Use after free in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-11692	Use after free in Read Anything in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-11635	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-10889	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-11631	Use after free in Aura in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-11700	Use after free in Tracing in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-10908	Use after free in FullScreen in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-41011	PackagePersister.validate_tgz builds "tar -tf #{tgz} 2>&1" where tgz = File.join(release_dir, 'packages', "#{name}.tgz") and name = package_meta['name'] comes directly from release.MF inside the uploaded tarball. The string is passed to Bosh::Common::Exec.sh, which executes via %x{} — i.e., /bin/sh -c. No Shellwords.escape is applied. The Models::Package Sequel validation (VALID_ID = /^[-0-9A-Za-z_+.]+$/i) would reject the name, but in create_package (lines 74–79) the shell-out in save_package_source_blob runs before package.save, so validation fires too late. Affected versions: - BOSH: all versions prior to v282.1.12 (inclusive); fixed in v282.1.12 or later	8.2	More Details
CVE-2019-25726	All in One Video Downloader 1.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send requests to the admin interface with UNION-based SQL injection payloads in the id parameter to extract sensitive database information including usernames, databases, and version details.	8.2	More Details
CVE-2016-20062	Simply Poll 1.4.1 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through the 'pollid' POST parameter. Attackers can send requests to the admin-ajax.php endpoint with the 'spAjaxResults' action and malicious 'pollid' values to execute arbitrary SQL queries and read sensitive data from the WordPress database.	8.2	More Details
CVE-2016-20065	Product Catalog 8 1.2 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the selectedCategory parameter. Attackers can submit POST requests to the admin-ajax.php endpoint with	8.2	More Details

	the UpdateCategoryList action to extract sensitive database information from WordPress tables.		
CVE-2026-41010	ReleaseJob#unpack builds job_dir = File.join(@release_dir, 'jobs', name) and job_tgz = File.join(@release_dir, 'jobs', "#{name}.tgz") where name returns @job_meta['name'], a value taken verbatim from the jobs: array of the attacker-supplied release.MF inside the uploaded tarball. These paths are then interpolated into a shell string: Bosh::Common::Exec.sh("tar -C #{job_dir} -xf #{job_tgz} 2>&1", :on_error => :return). Bosh::Common::Exec.sh executes via %x{#{command}} (bosh-common/lib/bosh/common/exec.rb:53), i.e. /bin/sh -c, so any shell metacharacters in name are interpreted. FileUtils.mkdir_p(job_dir) on line 49 creates the literal directory (no shell) and succeeds even when the name contains $()/;, so execution reaches the sh call. Affected versions: - BOSH Director: all versions prior to v282.1.12 (inclusive); fixed in v282.1.12 or later	8.2	More Details
CVE-2026-45476	Use after free in Linux MANA Driver allows an authorized attacker to elevate privileges locally.	8.2	More Details
CVE-2026-47907	Dreamweaver Desktop versions 21.7 and earlier are affected by an Improper Access Control vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	8.2	More Details
CVE-2026-44822	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	8.2	More Details
CVE-2026-50205	System log files output unencrypted SMTP server authentication passwords alongside sensitive employee corporate identification data.	8.2	More Details
CVE-2026-41249	CoreShop is a Pimcore enhanced eCommerce solution. In versions 5.0.1 through 5.1.0-beta.1,, the GitHub Actions workflow (`.github/workflows/static.yml`) uses the `pull_request_target` trigger but dangerously checks out the unverified code from the pull request head (`ref: ${{ github.event.pull_request.head.ref }}`). Subsequently, it executes a script (`bin/console`) from this untrusted checkout. This allows any external attacker to achieve Remote Code Execution (RCE) on the GitHub Actions runner simply by submitting a malicious Pull Request. Also known as a "Pwn Request" vulnerability. As of time of publication, `pull_request_target` is still in the file.	8.2	More Details
CVE-2023-29146	The utility functions used by Malwarebytes EDR 1.0.11 on Linux for calculating a cryptographic hash of data bytes truncate the hashed data if it exceeds 4GB. This leads to an integer wrap-around if the data is larger than the maximum unsigned integer value (32-bit). Attackers could create a colliding hash value for two different strings by attaching 4GB of data to a string that is less than 4GB in size.	8.2	More Details
CVE-2026-45327	TinyIce is a streaming server for audio and video. In versions 0.8.95 through 2.4.1, missing authentication on WebRTC ingest endpoint allows unauthenticated stream injection. Version 2.5.0 fixes the issue by requiring either HTTP Basic auth or a `?password=` query parameter, comparing the supplied password against the per-mount source password (or the `default_source_password` fallback) using bcrypt, hooking into the existing brute-force IP rate-limiter (5 failed attempts per IP within 15 minutes triggers a lockout), and rejecting requests for mounts in `disabled_mounts`. The same release also tightens an adjacent endpoint, `POST /admin/golive/chunk`, which previously required session authentication but did not verify the session user's per-mount access nor check the CSRF token.	8.2	More Details
CVE-2019-25745	WordPress Plugin Google Review Slider 6.1 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'tid' parameter. Attackers can send GET requests to the admin interface with malicious 'tid' values to extract sensitive database information using time-based blind SQL injection techniques.	8.2	More Details
CVE-2017-20249	Apptha Slider Gallery 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the albid parameter. Attackers can send GET requests with crafted SQL payloads in the albid parameter to extract sensitive database information including user credentials and authentication hashes.	8.2	More Details
CVE-2017-20245	Wow Viral Signups 2.1 WordPress plugin contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by exploiting the unescaped 'idsignup' POST parameter. Attackers can send crafted requests to the admin-ajax.php endpoint with malicious SQL payloads in the 'idsignup' parameter to read arbitrary data from the database.	8.2	More Details
CVE-2019-25728	Care2x 2.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL commands by manipulating the ck_config cookie parameter. Attackers can inject malicious SQL through the ck_config cookie in multiple endpoints including login.php, indexframe.php, and various module files to extract sensitive database information without authentication.	8.2	More Details

CVE-2026-47652	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	8.2	More Details
CVE-2019-25730	Listing Hub CMS 1.0 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to pages.php with crafted id values using error-based SQL injection techniques to extract database credentials, usernames, and version information.	8.2	More Details
CVE-2025-69755	An issue in Neterbit NW-431F Router vNW-431F-20241014-IR03 allows a remote attacker to obtain sensitive information and execute arbitrary code via a crafted command to the at_command.asp interface	8.2	More Details
CVE-2017-20246	KittyCatfish 2.2 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to read database contents by exploiting an unescaped GET parameter. Attackers can inject SQL code through the 'kc_ad' parameter in base.css.php or kittycatfish.php to extract sensitive database information using boolean-based blind or time-based blind techniques.	8.2	More Details
CVE-2019-25732	PHP EI-Tube Script 3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the search parameter. Attackers can send GET requests to the search endpoint with crafted SQL payloads in the query parameter to extract sensitive database information including usernames, passwords, and version details.	8.2	More Details
CVE-2017-20247	WordPress Plugin PICA Photo Gallery 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the aid parameter. Attackers can send GET requests with crafted SQL payloads in the aid parameter to extract sensitive database information including user credentials and table contents.	8.2	More Details
CVE-2017-20244	Wow Forms WordPress Plugin version 2.1 contains an SQL injection vulnerability that allows unauthenticated attackers to read arbitrary database information by exploiting an unescaped POST parameter. Attackers can inject SQL code through the 'mwpformid' parameter in requests to the admin-ajax.php endpoint with the 'send_mwp_form' action to extract sensitive database contents.	8.2	More Details
CVE-2017-20243	WordPress Car Park Booking Plugin version 13 October 17 contains a time-based SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the space_id parameter. Attackers can send GET requests to the booking-page endpoint with malicious space_id values using AND SLEEP() payloads to extract sensitive database information.	8.2	More Details
CVE-2026-11111	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-35081	The ugw-logstop method allows a remote attacker with user privileges to terminate arbitrary processes due to insufficient validation of user-supplied input.	8.1	More Details
CVE-2026-35080	The ugw-restoreinfo method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	8.1	More Details
CVE-2026-11015	Out of bounds read in WebGPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-35079	The ugw-restore method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	8.1	More Details
CVE-2026-35076	The bac-scanresult method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	8.1	More Details
CVE-2026-35077	The ugw-delete-file method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	8.1	More Details
CVE-2026-47631	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	8.1	More Details
CVE-	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 exposes 15 of 18 UPnP IGD actions		

2026-36603	without authentication on port 1900, including AddPortMapping and GetExternalIPAddress. UPnP is enabled by default through the admin interface, allowing any unauthenticated LAN device to create arbitrary port forwarding rules and access WAN traffic statistics.	8.1	More Details
CVE-2026-45635	Use after free in Universal Plug and Play (upnp.dll) allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-11693	Inappropriate implementation in Plugins in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-41855	In an untrusted JMS environment, org.springframework.jms.support.converter.MappingJackson2MessageConverter and org.springframework.jms.support.converter.JacksonJsonMessageConverter allow arbitrary class instantiation, which can lead to unauthorized actions via gadget class deserialization. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	8.1	More Details
CVE-2026-10863	A security issue was fixed in the correlations over-correlation endpoint where the order query parameter was accepted from user-controlled named request parameters. This allowed an authenticated user to override the server-defined ordering of over-correlating values. Depending on how the value was processed by the underlying data access layer, this could allow manipulation of database query ordering and potentially expose the application to unsafe query construction. The patch removes order from the set of request-controlled parameters and instead sets the ordering server-side to occurrence desc after processing allowed user parameters. Affected component: app/Controller/CorrelationsController.php, overCorrelations() Security impact: An authenticated attacker could influence the ordering clause used by the over-correlations query. The direct impact appears limited to query manipulation unless further evidence confirms SQL injection or unauthorized data exposure through the manipulated ordering expression.	8.1	More Details
CVE-2026-10930	Out of bounds read in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-24065	Waves Central for macOS versions 13.0.9 through 16.5.5 contain a local privilege escalation vulnerability in the privileged helper service. The helper validates connecting XPC clients using the client process identifier (PID) to verify code-signing identity. Because process identifiers can be reused, a local attacker can exploit a race condition between the time a connection request is made and the time the helper performs validation, causing the helper to trust an attacker-controlled process. This allows the attacker to invoke privileged operations, resulting in arbitrary code execution as root. The issue is fixed in version 16.6.2.	8.1	More Details
CVE-2026-42974	Integer underflow (wrap or wraparound) in Windows Performance Monitor allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-11185	Use after free in V8 in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-11643	Use after free in Proxy in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	8.1	More Details
CVE-2026-11689	Insufficient policy enforcement in Passwords in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2026-11416	MoviePilot contains a path traversal vulnerability in the AliPan, U115, and Rclone cloud storage download handlers where the local destination path is constructed by concatenating the configured download directory with a filename taken directly from remote cloud API metadata without basename normalization or path validation. An attacker who controls a filename returned by a remote cloud storage API can include traversal sequences ../ in the filename to cause downloaded content to be written outside the configured download directory, potentially overwriting arbitrary files including configuration or plugin files reachable by the application process.	8.1	More Details
CVE-2026-42981	Integer underflow (wrap or wraparound) in Windows Performance Monitor allows an unauthorized attacker to execute code over a network.	8.1	More Details

CVE-2026-7383	Issue summary: A signed integer overflow when sizing the destination buffer for Unicode output in ASN1_mbstring_ncopy() can lead to a heap buffer overflow. Impact summary: A heap buffer overflow may lead to a crash or possibly attacker controlled code execution or other undefined behaviour. In ASN1_mbstring_copy() and ASN1_mbstring_ncopy() the destination size for Unicode output is computed in a signed int: by left shift of the input character count for BMPSTRING (UTF-16) and UNIVERSALSTRING (UTF-32), and by summing per-character byte counts for UTF8STRING. The calculation overflows when the input reaches around 2^30 characters. In the worst case (UNIVERSALSTRING at 2^30 characters) the size wraps to zero, OPENSSL_malloc(1) is called, and the subsequent character copy writes several gigabytes past the one-byte allocation. X.509 certificate processing routes through ASN1_STRING_set_by_NID(), whose DIRSTRING_TYPE mask excludes UNIVERSALSTRING and whose per-NID size limits cap the input length; no network protocol or certificate-handling path in OpenSSL exercises the overflow. Triggering the bug requires an application that calls ASN1_mbstring_copy() or ASN1_mbstring_ncopy() directly, or registers a custom string type via ASN1_STRING_TABLE_add(), with attacker-controlled input on the order of half a gigabyte or more. For these reasons this issue was assigned Low severity. The FIPS modules in 4.0, 3.6, 3.5, 3.4 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	8.1	More Details
CVE-2026-9662	The Recover Exit For WooCommerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to and including 1.0.3. This is due to insufficient validation and sanitization of the user-controlled `tpf` POST parameter before it is used in an `include()` path in the `recover_exit()` function. This makes it possible for unauthenticated attackers to perform path traversal and include unintended local PHP files, which can lead to sensitive information exposure and, in certain deployment chains, code execution.	8.1	More Details
CVE-2026-36720	Insecure permissions in bookcars v8.3 allows authenticated attackers to escalate privileges from user to admin via modifying their user type.	8.1	More Details
CVE-2026-47930	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue does not require user interaction.	8.1	More Details
CVE-2026-11169	Inappropriate implementation in XML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted XML file. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-46484	Headplane is a feature-complete Web UI for Headscale. Prior to versions 0.6.3 and 0.7.0-beta.3, Headplane was vulnerable to a path traversal / authorization bypass in the Headscale API client used by node and user rename operations. This issue has been patched in versions 0.6.3 and 0.7.0-beta.3.	8.1	More Details
CVE-2026-45599	Use after free in Universal Plug and Play (upnp.dll) allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-11224	Use after free in Chromoting in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Low)	8.1	More Details
CVE-2026-9753	The $_internalApplyOplogUpdate aggregation pipeline stage can be used to execute a document diff containing a malformed binary diff to return memory out-of-bounds or crash the server. $_internalApplyOplogUpdate can be executed by any authenticated user with access to the aggregate command.	8.1	More Details
CVE-2026-45743	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. 16 file-manager endpoints in Termix prior to version 2.3.2 do not verify that the requesting user owns the SSH session identified by `sessionId`. An authenticated attacker who knows or guesses another user's active `sessionId` can read, write, delete, download, and execute files on the victim's connected SSH host. Version 2.3.2 patches the issue.	8.1	More Details
CVE-2026-45749	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. The `POST /users/totp/disable` and `POST /users/totp/backup-codes` endpoints in Termix prior to version 2.3.2 accept the account password as a sole authentication factor for MFA-critical operations. An attacker who obtains a user's password (phishing, credential stuffing, the passwordHash leak in GHSA-xxxx) can disable TOTP entirely or regenerate backup codes, without ever possessing the TOTP device or knowing a valid TOTP code. This renders two-factor authentication ineffective. Version 2.3.2 patches the issue.	8.1	More Details
CVE-2026-	Improper neutralization of special elements in output used by a downstream component ('injection') in Microsoft Teams for Android allows an authorized attacker to disclose information over a network.	8.1	More Details

42835			
CVE-2026-11011	Insufficient policy enforcement in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-49948	Mem0 versions through 0.2.8, fixed in commit ae7f406, contain a missing authorization vulnerability in the self-hosted server component where the POST /configure endpoint modifies global LLM provider and embedder configuration but only verifies authentication via JWT or X-API-Key without validating the caller's role. Any authenticated user holding a distributed API key can redirect all LLM and embedder traffic to an attacker-controlled server, with the malicious configuration persisted to PostgreSQL and surviving server restarts to affect all users and API keys on the instance.	8.1	More Details
CVE-2026-45503	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to disclose information over a network.	8.1	More Details
CVE-2026-42987	Use after free in Windows Deployment Services allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2025-59874	HCL Hive Telco Observability is affected by a Required directives missing from the CSP issue is detected in keycloak component of the web application. Missing essential directives can leave a site vulnerable.	8.1	More Details
CVE-2026-11231	Inappropriate implementation in Safe Browsing in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a malicious file. (Chromium security severity: Low)	8.1	More Details
CVE-2026-11170	Inappropriate implementation in Chromoting in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to perform OS-level privilege escalation via malicious network traffic. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-35078	The ugw-logstop method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	8.1	More Details
CVE-2026-10887	Use after free in Chromoting in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	8.1	More Details
CVE-2026-41723	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	8.0	More Details
CVE-2026-41722	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	8.0	More Details
CVE-2026-47298	Improper authorization in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2026-11241	Insufficient validation of untrusted input in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	8.0	More Details
CVE-2026-45644	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Live Share Canvas SDK allows an authorized attacker to elevate privileges over a network.	8.0	More Details
CVE-2026-45745	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Starting in version 1.7.0, Termix Desktop (Electron) disables TLS certificate validation, allowing a machine-in-the-middle attacker to intercept and modify HTTPS traffic to the configured Termix server. This can lead to credential theft and JWT/session theft during login and normal use. As of time of publication, no known patched versions are available.	8.0	More Details
CVE-2026-41724	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	8.0	More Details
	An untrusted search path issue in the GlobalDatabasePlugin in the AWS Advanced Go Wrapper for		

CVE-2026-11401	Amazon Aurora PostgreSQL will allow a remote authenticated low-privilege actor to escalate privileges to those of another Amazon RDS user, including rds_superuser, via a crafted function created by the actor that runs when that user connects to the cluster through the affected wrapper. To remediate this issue, users should upgrade to the AWS Advanced Go Wrapper release 2026-05-26	8.0	More Details
CVE-2026-11400	An untrusted search path issue in the GlobalDatabasePlugin in the AWS Advanced JDBC Wrapper for Amazon Aurora PostgreSQL will allow a remote authenticated low-privilege actor to escalate privileges to those of another Amazon RDS user, including rds_superuser, via a crafted function created by the actor that runs when that user connects to the cluster through an affected wrapper. To remediate this issue, users should upgrade to AWS Advanced JDBC Wrapper version 4.0.1.	8.0	More Details
CVE-2026-34693	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	8.0	More Details
CVE-2025-14773	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	8.0	More Details
CVE-2026-48575	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-48573	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-45654	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-48568	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-48570	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-47656	Protection mechanism failure in Windows Boot Manager allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-45588	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-48576	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-48578	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	7.9	More Details
CVE-2026-44812	Integer overflow or wraparound in Windows Win32K - GRFX allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-21029	Improper export of android application components in Galaxy Editing Service prior to SMR Jun-2026 Release 1 allows local attacker to execute privileged operations.	7.8	More Details
CVE-2026-34698	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: power: supply: pm8916_lbc: Fix use-after-free for extcon in IRQ handler Using the `devm_` variant for requesting IRQ _before_ the `devm_`		

CVE-2026-46246	variant for allocating/registering the `extcon` handle, means that the `extcon` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `extcon` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `extcon_set_state_sync()` with a freed `extcon` handle. Which usually crashes the system or otherwise silently corrupts the memory... Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `extcon` handle.	7.8	More Details
CVE-2026-11822	SQLite before 3.53.2 contains memory corruption vulnerabilities in the FTS5 full-text search extension that allow attackers to cause process crashes, memory exhaustion, or arbitrary code execution by supplying a crafted database with malformed FTS5 page data. Attackers can trigger an out-of-bounds read in fts5LeafSeek() via an attacker-controlled loop bound and a heap buffer overflow write in fts5ChunkIterate() through a crafted continuation page causing an integer underflow, exploitable when an FTS5 MATCH query is executed against the malicious database.	7.8	More Details
CVE-2026-49161	Improper access control in Microsoft PC Manager allows an authorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-47292	Inclusion of functionality from untrusted control sphere in Visual Studio Code allows an unauthorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-46253	In the Linux kernel, the following vulnerability has been resolved: pstore/ram: fix buffer overflow in persistent_ram_save_old() persistent_ram_save_old() can be called multiple times for the same persistent_ram_zone (e.g., via ramoops_pstore_read -> ramoops_get_next_prz for PSTORE_TYPE_DMESG records). Currently, the function only allocates prz->old_log when it is NULL, but it unconditionally updates prz->old_log_size to the current buffer size and then performs memcpy_fromio() using this new size. If the buffer size has grown since the first allocation (which can happen across different kernel boot cycles), this leads to: 1. A heap buffer overflow (OOB write) in the memcpy_fromio() calls 2. A subsequent OOB read when ramoops_pstore_read() accesses the buffer using the incorrect (larger) old_log_size The KASAN splat would look similar to: BUG: KASAN: slab-out-of-bounds in ramoops_pstore_read+0x... Read of size N at addr ... by task ... The conditions are likely extremely hard to hit: 0. Crash with a ramoops write of less-than-record-max-size bytes. 1. Reboot: ramoops registers, pstore_get_records(0) reads old crash, allocates old_log with size X 2. Crash handler registered, timer started (if pstore_update_ms >= 0) 3. Oops happens (non-fatal, system continues) 4. pstore_dump() writes oops via ramoops_pstore_write() size Y (>X) 5. pstore_new_entry = 1, pstore_timer_kick() called 6. System continues running (not a panic oops) 7. Timer fires after pstore_update_ms milliseconds 8. pstore_timefunc() → schedule_work() → pstore_dowork() → pstore_get_records(1) 9. ramoops_get_next_prz() → persistent_ram_save_old() 10. buffer_size() returns Y, but old_log is X bytes 11. Y > X: memcpy_fromio() overflows heap Requirements: - a prior crash record exists that did not fill the record size (almost impossible since the crash handler writes as much as it can possibly fit into the record, capped by max record size and the kmsg buffer almost always exceeds the max record size) - pstore_update_ms >= 0 (disabled by default) - Non-fatal oops (system survives) Free and reallocate the buffer when the new size differs from the previously allocated size. This ensures old_log always has sufficient space for the data being copied.	7.8	More Details
CVE-2026-34710	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-50261	A use-after-free flaw was found in the X.Org X server and Xwayland in SyncChangeCounter(). A client that sets up multiple SyncCounters can trigger a use-after-free when destroying those counters via a second client connection while changing those counters. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-49189	Unchecked public access permissions on a core Broadcast Receiver allow unauthorized local software components to invoke administrative operations.	7.8	More Details
CVE-2026-50260	A use-after-free flaw was found in the X.Org X server and Xwayland in FreeCounter(). A client that sets up multiple SyncCounters and awaits on those triggers can trigger a use-after-free when destroying those counters via a second client connection. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-44811	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability		More

2026-34709	that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	Details
CVE-2026-8863	Multiple Microsoft-sigend UEFI SHIM bootloaders are vulnerable to SecureBoot bypass. An attacker with administrative privileges or the ability to modify the boot process could use one of the vulnerable shim bootloaders to bypass Secure Boot protections and execute arbitrary code before the operating system loads. Specific UEFI DBX update is required to block these vulnerable boot loaders.	7.8	More Details
CVE-2026-11824	SQLite before 3.53.2 contains a heap-based buffer overflow vulnerability in the FTS5 full-text search extension that allows attackers to cause a crash or execute arbitrary code by supplying a crafted database with malicious continuation page metadata specifying a szLeaf value smaller than 4. Attackers can trigger an integer underflow in fts5ChunkIterate() causing an inflated remaining byte count during FTS5 MATCH query processing, leading to a heap buffer overflow of attacker-controlled data in applications compiled with SQLITE_ENABLE_FTS5.	7.8	More Details
CVE-2026-50264	An out-of-bounds write flaw was found in the X.Org X server and Xwayland in DRIGetBuffers/DRIGetBuffersWithFormat. A client that requests multiple DRI2BufferBackLeft attachments and one DRI2BufferFrontLeft can trigger an out-of-bounds heap write. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-44809	Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-11332	A flaw was found in ansible-core. The ansible-galaxy role install command processes dependency specifications from a role's meta/requirements.yml file. Due to improper neutralization of argument delimiters, a malicious role author can inject arbitrary git configuration flags through the src field. This allows arbitrary code execution on the machine of a user who installs the role via ansible-galaxy role install.	7.8	More Details
CVE-2022-49036	An inclusion of functionality from untrusted control sphere vulnerability in OpenSSL configuration in Synology Active Backup for Business Recovery Media Creator before 2.5.0-2081 allows local users to execute arbitrary code via unspecified vectors.	7.8	More Details
CVE-2026-40290	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.16.0 and prior to 4.11.0, a user-after-free (UAF) race condition exists in the shared memory teardown logic of FF-A within OP-TEE SPMC/SP flows. This only applies when OP-TEE is configured as an SPMC for S-EL0 SPs, that is, with `CFG_SECURE_PARTITION=y`. The function `sp_mem_remove()`, responsible for freeing entries in `smem->receivers` and `smem->regions`, fails to acquire the global `sp_mem_lock` before performing the `free()` operations. Concurrently, other code paths, such as `sp_mem_get_receiver()`, iterate over these same lists without holding a lock, or, like `sp_mem_is_shared()`, iterate while holding the lock but are not serialized against the unprotected `free()` in `sp_mem_remove()`. This creates a cross-thread race where a thread iterating the list can acquire a pointer to an entry (e.g., `struct sp_mem_map_region` or `struct sp_mem_receiver`), and then another thread calls `sp_mem_remove()`, freeing the object. When the first thread resumes and dereferences the pointer, it results in a Use-After-Free vulnerability. Version 4.11.0 fixes the issue.	7.8	More Details
CVE-2026-36574	A DLL hijacking vulnerability in Wassimulator (GitHub) CactusViewer v2.3.0 allows attackers to escalate privileges and execute arbitrary code via a crafted DLL.	7.8	More Details
CVE-2026-47918	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-44823	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-47919	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47920	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47921	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE-2026-45471	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-48565	Untrusted search path in Windows Narrator Braille allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45469	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-50209	Broadcast events allow malicious software to rewrite the device's default Mobile Device Management (MDM) endpoint address, shifting administrative ownership to an external attacker.	7.8	More Details
CVE-2026-11103	Inappropriate implementation in Installer in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2026-50207	The system Binder boundary accepts unverified pass-through AT commands, giving local applications the power to read baseband files or disable cellular connectivity.	7.8	More Details
CVE-2026-44824	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-47952	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47955	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34697	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47959	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-48292	Format Plugins versions 1.1.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-48291	Format Plugins versions 1.1.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47917	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47916	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-44813	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-34695	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47908	Dreamweaver Desktop versions 21.7 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE-2026-21030	Improper access control in MediaTek Audio HAL prior to SMR Jun-2026 Release 1 allows local attackers to trigger privileged functions.	7.8	More Details
CVE-2026-48305	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-45475	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-48306	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-11072	Use after free in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to execute arbitrary code via a malicious file. (Chromium security severity: Medium)	7.8	More Details
CVE-2026-44817	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-44819	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-50259	A stack-based buffer overflow flaw was found in the X.Org X server and Xwayland. _XkbSetMapChecks() declares a fixed-size stack buffer mapWidths[256] indexed by key type index. The helper function CheckKeyTypes() writes to this buffer at a client-controlled offset, allowing a stack buffer overflow. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-47915	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-49042	An inclusion of functionality from untrusted control sphere vulnerability in MinGW DLL component in Synology Hyper Backup Explorer before 3.0.1-0156 allows local users to execute arbitrary code via unspecified vectors.	7.8	More Details
CVE-2026-44820	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-47911	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21031	Improper authorization in AppBlock prior to SMR Jun-2026 Release 1 allows local attacker to launch arbitrary activity. User interaction is required for triggering this vulnerability.	7.8	More Details
CVE-2026-47912	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47913	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34696	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-47914	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details

44808			
CVE-2026-45605	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45486	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-34699	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-45637	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45638	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-34700	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-50511	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-50512	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-41092	Improper access control in Microsoft Kinect allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-40409	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2026-44807	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-40404	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2026-45645	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-45457	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-45643	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-48574	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-42977	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-	Inappropriate implementation in UI in Google Chrome on Windows prior to 149.0.7827.53 allowed a local	7.8	More

10942	attacker to perform privilege escalation via a malicious file. (Chromium security severity: High)		Details
CVE-2026-42978	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42979	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42980	Integer underflow (wrap or wraparound) in Windows NT OS Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-48293	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-42916	Integer underflow (wrap or wraparound) in Windows NT OS Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45636	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-50256	A stack-based buffer overflow flaw was found in the X.Org X server and Xwayland. A mismatch between the X server and the libXfont2 library's maximum font name length can cause a stack buffer overflow during font alias resolution. The server allocates a 256 byte stack buffer but libXfont2's alias target name length is 1024 bytes. A font alias name between 257 and 1023 bytes causes the X server to copy that name into the undersized stack buffer without further checks. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-45600	Access of resource using incompatible type ('type confusion') in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42828	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42829	Improper access control in Windows Administrator Protection allows an authorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-45593	Use after free in Windows SDK allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45592	Integer overflow or wraparound in Windows Internet (wininet.dll) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42837	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45586	Improper link resolution before file access ('link following') in Windows Collaborative Translation Framework allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42902	Improper authorization in Microsoft PowerToys allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42905	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
	A network man-in-the-middle between nats-sync and the BOSH director can steal the director credentials (Basic auth header or UAA client secret) and can tamper with the VM list that is written into the NATS		

CVE-2026-41859	authorization file. Stolen credentials grant administrative director access. UsersSync#bosh_api_response_body builds a Net::HTTP client with verify_mode = OpenSSL::SSL::VERIFY_NONE for every director call (/info, /deployments, /deployments/<name>/vms). Affected versions: - BOSH: all versions prior to v282.1.9 (inclusive); fixed in v282.1.9 or later	7.8	More Details
CVE-2026-34701	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34702	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-25551	Seagull Software BarTender 2021 R1 through 12.0.1 contains an insecure deserialization vulnerability that allows low-privileged local users to escalate privileges. The DataServiceSingleton .NET Remoting endpoint is bound to localhost on TCP port 7375 via BtSystem.Service.exe, limiting the attack surface to local access only. The endpoint is configured with BinaryServerFormatterSinkProvider and TypeFilterLevel set to Full. A low-privileged local attacker can send YSoSerial.NET-generated BinaryFormatter payloads to the localhost-bound endpoint to achieve code execution as NT AUTHORITY\\SYSTEM.	7.8	More Details
CVE-2026-42910	Out-of-bounds write in Windows Hotpatch Monitoring Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-34706	InCopy versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34707	InCopy versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34708	InCopy versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-42983	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-50257	A use-after-free flaw was found in the X.Org X server and Xwayland in miSyncDestroyFence(). A client that sets up multiple fence triggers can trigger a use-after-free function pointer call. An attacker would connect to the X server to set up a fence and await that fence, then a second X connection destroys the fence, causing the use-after-free. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-46259	In the Linux kernel, the following vulnerability has been resolved: procfs: fix missing RCU protection when reading real_parent in do_task_stat() When reading /proc/[pid]/stat, do_task_stat() accesses task->real_parent without proper RCU protection, which leads to: cpu 0 cpu 1 ----- ----- do_task_stat var = task->real_parent release_task call_rcu(delayed_put_task_struct) task_tgid_nr_ns(var) rcu_read_lock <--- Too late to protect task->real_parent! task_pid_ptr <--- UAF! rcu_read_unlock This patch uses task_ppid_nr_ns() instead of task_tgid_nr_ns() to add proper RCU protection for accessing task->real_parent.	7.8	More Details
CVE-2026-44804	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45658	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	7.8	More Details
CVE-2026-44802	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	7.8	More Details
	A vulnerability in the CLI of Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, and Cisco Catalyst SD-WAN Validator, formerly SD-WAN vBond, could allow an authenticated, local attacker to execute arbitrary commands as root by supplying a crafted file to the affected system. This vulnerability is due to insufficient validation of user-supplied		

CVE-2026-20245	input. An attacker could exploit this vulnerability by uploading a crafted file to the affected system. A successful exploit could allow the attacker to perform command injection attacks on an affected system and elevate their privileges as the root user. To exploit this vulnerability, the attacker must have netadmin privileges on the affected system. This would require valid credentials or exploitation of or . Cisco is not aware of successful exploitation by other methods. Cisco has observed limited cases where the exploitation of this bug resulted in a configuration change pushed to edge devices. Cisco recommends that customers upgrade to the fixed software that is documented in the that was published on May 14, 2026, and verify the configuration of the edge devices.	7.8	More Details
CVE-2026-45656	Protection mechanism failure in Windows UEFI allows an authorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-46271	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: do WoW offloads only on primary link In case of multi-link connection, WCN7850 firmware crashes due to WoW offloads enabled on both primary and secondary links. Change to do it only on primary link to fix it. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1.c5-00284-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1	7.8	More Details
CVE-2026-33828	Trust boundary violation in Windows Attestation allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-45490	Improper authorization in .NET allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-50258	A stack-based buffer overflow flaw was found in the X.Org X server and Xwayland. The X server has multiple stack buffers sized XkbMaxShiftLevel * XkbNumKbdGroups but CheckKeyTypes() does not verify or clamp non-canonical key types to XkbMaxShiftLevel. A client can change key types to excessive shift levels and trigger stack overflows. This is caused by an incomplete fix of CVE-2025-26597. This may be used to crash the server, or for privilege escalation if the X server runs as root.	7.8	More Details
CVE-2026-48583	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-46263	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix out-of-bounds stream encoder index v3 eng_id can be negative and that stream_enc_regs[] can be indexed out of bounds. eng_id is used directly as an index into stream_enc_regs[], which has only 5 entries. When eng_id is 5 (ENGINE_ID_DIGF) or negative, this can access memory past the end of the array. Add a bounds check using ARRAY_SIZE() before using eng_id as an index. The unsigned cast also rejects negative values. This avoids out-of-bounds access. Fixes the below smatch error: dcn*_resource.c: stream_encoder_create() may index stream_enc_regs[eng_id] out of bounds (size 5). drivers/gpu/drm/amd/amdgpu/../display/dc/resource/dcn351/dcn351_resource.c 1246 static struct stream_encoder *dcn35_stream_encoder_create(1247 enum engine_id eng_id, 1248 struct dc_context *ctx) 1249 { ... 1255 1256 /* Mapping of VPG, AFMT, DME register blocks to DIO block instance */ 1257 if (eng_id <= ENGINE_ID_DIGF) { ENGINE_ID_DIGF is 5. should <= be <? Unrelated but, ugh, why is Smatch saying that "eng_id" can be negative? end_id is type signed long, but there are checks in the caller which prevent it from being negative. 1258 vpg_inst = eng_id; 1259 afmt_inst = eng_id; 1260 } else 1261 return NULL; 1262 ... 1281 1282 dcn35_dio_stream_encoder_construct(enc1, ctx, ctx->dc_bios, 1283 eng_id, vpg, afmt, --> 1284 &stream_enc_regs[eng_id], ^^^^^^^^^^^^^^^^^^^^^^^^^^ This stream_enc_regs[] array has 5 elements so we are one element beyond the end of the array. ... 1287 return &enc1->base; 1288 } v2: use explicit bounds check as suggested by Roman/Dan; avoid unsigned int cast v3: The compiler already knows how to compare the two values, so the cast (int) is not needed. (Roman)	7.8	More Details
CVE-2026-44803	Integer overflow or wraparound in Windows Win32K - GRFX allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-42991	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-46267	In the Linux kernel, the following vulnerability has been resolved: nfc: hci: shdlc: Stop timers and work before freeing context llc_shdlc_deinit() purges SHDLC skb queues and frees the llc_shdlc structure while its timers and state machine work may still be active. Timer callbacks can schedule sm_work, and sm_work accesses SHDLC state and the skb queues. If teardown happens in parallel with a queued/running work item, it can lead to UAF and other shutdown races. Stop all SHDLC timers and cancel sm_work synchronously before purging the queues and freeing the context. Found by Linux	7.8	More Details

	Verification Center (linuxtesting.org) with SVACE.		
CVE-2026-42986	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-46260	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix out-of-bound access in fib6_add_rt2node(). syzbot reported out-of-bound read in fib6_add_rt2node(). [0] When IPv6 route is created with RTA_NH_ID, struct fib6_info does not have the trailing struct fib6_nh. The cited commit started to check !iter->fib6_nh->fib_nh_gw_family to ensure that rt6_qualify_for_ecmp() will return false for iter. If iter->nh is not NULL, rt6_qualify_for_ecmp() returns false anyway. Let's check iter->nh before reading iter->fib6_nh and avoid OOB read. [0]: BUG: KASAN: slab-out-of-bounds in fib6_add_rt2node+0x349c/0x3500 net/ipv6/ip6_fib.c:1142 Read of size 1 at addr ffff8880384ba6de by task syz.0.18/5500 CPU: 0 UID: 0 PID: 5500 Comm: syz.0.18 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 Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xba/0x230 mm/kasan/report.c:482 kasan_report+0x117/0x150 mm/kasan/report.c:595 fib6_add_rt2node+0x349c/0x3500 net/ipv6/ip6_fib.c:1142 fib6_add_rt2node_nh net/ipv6/ip6_fib.c:1363 [inline] fib6_add+0x910/0x18c0 net/ipv6/ip6_fib.c:1531 __ip6_ins_rt net/ipv6/route.c:1351 [inline] ip6_route_add+0xde/0x1b0 net/ipv6/route.c:3957 inet6_rtm_newroute+0x268/0x19e0 net/ipv6/route.c:5660 rtnetlink_rcv_msg+0x7d5/0xbe0 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592 ___sys_sendmsg+0x2a5/0x360 net/socket.c:2646 __sys_sendmsg net/socket.c:2678 [inline] __do_sys_sendmsg net/socket.c:2683 [inline] __se_sys_sendmsg net/socket.c:2681 [inline] __x64_sys_sendmsg+0x1bd/0x2a0 net/socket.c:2681 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: 0033:0x7f9316b9aeb9 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:00007ffd8809b678 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f9316e15fa0 RCX: 00007f9316b9aeb9 RDX: 0000000000000000 RSI: 0000200000004380 RDI: 0000000000000003 RBP: 00007f9316c08c1f R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f9316e15fac R14: 00007f9316e15fa0 R15: 00007f9316e15fa0 </TASK> Allocated by task 5499: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 poison_kmalloc_redzone mm/kasan/common.c:398 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:415 kasan_kmalloc include/linux/kasan.h:263 [inline] __do_kmalloc_node mm/slub.c:5657 [inline] __kmalloc_noprof+0x40c/0x7e0 mm/slub.c:5669 kmalloc_noprof include/linux/slab.h:961 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] fib6_info_alloc+0x30/0xf0 net/ipv6/ip6_fib.c:155 ip6_route_info_create+0x142/0x860 net/ipv6/route.c:3820 ip6_route_add+0x49/0x1b0 net/ipv6/route.c:3949 inet6_rtm_newroute+0x268/0x19e0 net/ipv6/route.c:5660 rtnetlink_rcv_msg+0x7d5/0xbe0 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592 ___sys_s ---truncated---	7.8	More Details
CVE-2026-22926	Omnissa Workspace ONE® Assist for macOS contains a Local Privilege Escalation Vulnerability.	7.8	More Details
CVE-2026-45487	Time-of-check time-of-use (TOCTOU) race condition in Program Compatibility Assistant Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-42989	Improper link resolution before file access ('link following') in Winlogon allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-8795	A YAML injection vulnerability exists in the Windows.Collectors.Remapping artifact of Rapid7 Velociraptor before version 0.76.6. The hostname field in client_info.json inside a collection ZIP is inserted into a YAML template via Go's text/template without escaping. An attacker providing a crafted collection ZIP can leverage literal double quotes and newlines in the hostname to break out of the YAML quoted string and inject a new mount remapping entry. When an analyst applies the generated remapping file with --remap, arbitrary VQL executes on their machine with NullACLManager (all permissions granted, unsandboxed).	7.8	More Details

CVE-2026-11297	Insufficient validation of untrusted input in Reader Mode in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	7.7	More Details
CVE-2026-45497	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an authorized attacker to execute code over a network.	7.7	More Details
CVE-2026-49957	Hermes WebUI before version 0.51.269 contains a workspace boundary bypass vulnerability that allows authenticated attackers to circumvent blocked-root path checks by exploiting an early return in the SSH/remote terminal profile workspace resolution logic within _remote_terminal_workspace_candidate(). Attackers can configure a remote terminal working directory to a system directory such as /etc, causing the workspace resolution path to accept it as a trusted local workspace root before the _is_blocked_workspace_path() guard executes, enabling read access to local system files through workspace file-read helpers.	7.7	More Details
CVE-2026-4035	A vulnerability in mlflow/mlflow versions prior to 3.11.0 allows for the resolution of environment variables in AI Gateway secrets, which can be exploited to exfiltrate sensitive server-side environment credentials to an attacker-controlled endpoint. This issue arises because the `api_key` field in gateway secrets can accept `$ENV_VAR` references, which are resolved against the MLflow server's environment during runtime. The resolved secrets are then sent in provider authentication headers to the configured upstream `api_base`. This vulnerability can be exploited by low-privileged authenticated users in basic-auth deployments or by unauthenticated users in default deployments without `basic-auth`. The impact includes potential leakage of sensitive credentials such as cloud artifact credentials (`AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`), which could lead to artifact poisoning and cross-boundary code execution in downstream environments. The issue is fixed in version 3.11.0.	7.7	More Details
CVE-2026-5068	A remote, unauthenticated BLE peer can trigger a 2-byte out-of-bounds write in the Bluetooth host during L2CAP LE CoC SDU reassembly. When the application enables segmentation (via chan_ops.alloc_buf) and the chosen RX pool has a user_data_size smaller than 2 bytes, the segmentation counter stored in the net_buf user_data area is written out of bounds in l2cap_chan_le_recv_seg (subsys/bluetooth/host/l2cap.c). The observed effects are an AddressSanitizer abort and, without ASan, heap corruption / fatal error.	7.6	More Details
CVE-2026-49771	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in 10Web Photo Gallery by 10Web allows Blind SQL Injection. This issue affects Photo Gallery by 10Web: from n/a through 1.8.41.	7.6	More Details
CVE-2026-41518	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In versions 4.9.0 through 5.0.0, an authenticated user with project-editor permissions can store arbitrary HTML/JavaScript in the `ChartDatasetConfig.legend` field. The payload is persisted verbatim in the database, propagated through the Chart.js rendering pipeline, and injected into the tooltip DOM element via an unguarded `innerHTML` assignment in `ChartTooltip.js`. Every unauthenticated viewer of the public dashboard triggers JavaScript execution on page load — no hover interaction is required. Browser-based Playwright verification confirmed `alert('localhost')` fires immediately and `<img src="x" onerror="alert(document.domain)">` is present in the `#chartjs-tooltip` DOM element. Version 5.0.1 contains a fix.	7.6	More Details
CVE-2025-15655	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mojoomla School Management allows SQL Injection. This issue affects School Management: from n/a through 93.2.0.	7.6	More Details
CVE-2026-41234	Froxlor is open source server administration software. Prior to version 2.3.7, the `DomainZones.add` API endpoint does not sanitize newline characters in TXT record content. An authenticated customer with DNS editing enabled can inject newlines into TXT record values, which break out of the record line in the generated BIND zone file. This enables injection of arbitrary BIND directives (`$INCLUDE`, `$GENERATE`) and arbitrary DNS records (A, MX, CNAME) into the zone file written to disk by the DNS rebuild cron. This is an incomplete fix for CVE-2026-30932 (GHSA-x6w6-2xwp-3jh6), which patched the same newline injection for LOC, RP, SSHFP, and TLSA record types but did not patch TXT records. Version 2.3.7 contains an updated patch.	7.6	More Details
CVE-2026-41842	Spring MVC and WebFlux applications are vulnerable to Denial of Service (DoS) attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	7.5	More Details
CVE-2026-44801	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Integer		

2026-34711	Overflow or Wraparound vulnerability. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2026-34712	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Input Validation vulnerability. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2026-37460	Missing input validation in the rfapiRibBi2Ri() function (rfapi_rib.c) of FRRouting (FRR) stable/10.0 to stable/10.6 allows attackers to cause a Denial of Service (DoS) via supplying a crafted BGP UPDATE message.	7.5	More Details
CVE-2026-42570	Svelte devalue is a JavaScript library that serializes values into strings when JSON.stringify isn't sufficient for the job. From version 5.6.3 to before version 5.8.1, devalue.parse could, due to quirks in some JavaScript engines, be convinced to allocate much more memory than was needed when deserializing sparse arrays, leading to excessive memory consumption. This issue has been patched in version 5.8.1.	7.5	More Details
CVE-2026-42908	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-11296	Inappropriate implementation in ImageCapture in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-41850	Applications that evaluate user-supplied Spring Expression Language (SpEL) expressions are vulnerable to an Algorithmic Denial of Service (DoS). By providing a specially crafted expression, an attacker can trigger excessive resource consumption during evaluation, leading to application degradation or unavailability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	7.5	More Details
CVE-2026-42909	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-36501	An issue in the Externalizable.readExternal() component of Controller v12.0.5 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-41849	An integer overflow vulnerability exists in the evaluation logic of the Spring Expression Language (SpEL). An attacker can exploit this by supplying a specially crafted SpEL expression that triggers excessive resource consumption, resulting in a Denial of Service (DoS). Affected versions: Spring Framework 5.3.0 through 5.3.48.	7.5	More Details
CVE-2026-45445	Issue summary: When an application drives an AES-OCB context through the public EVP_Cipher() one-shot interface, the application-supplied initialisation vector (IV) is silently discarded. Impact summary: Every message encrypted under the same key uses the same effective nonce regardless of the IV supplied by the caller, resulting in (key, nonce) reuse and loss of confidentiality. If the same code path is used to compute the authentication tag, the tag depends only on the (key, IV) pair and not on the plaintext or ciphertext, allowing universal forgery of arbitrary ciphertext from a single captured message. OpenSSL provides two ways to drive a cipher: the documented streaming interface (EVP_CipherUpdate / EVP_CipherFinal_ex) and a lower-level one-shot, EVP_Cipher(), whose documentation explicitly recommends against use by applications in favour of EVP_CipherUpdate() and EVP_CipherFinal_ex(). The OCB provider's streaming handler flushes the application-supplied IV into the OCB context before processing data; the one-shot handler did not. Every call to EVP_Cipher() on an AES-OCB context therefore ran with the all-zero key-derived offset state left by cipher initialisation, regardless of the caller's IV. If EVP_EncryptFinal_ex() is subsequently used to obtain the authentication tag, the deferred IV setup runs at that point and clears the running checksum that should have been accumulated over the plaintext. The resulting tag is a function of (key, IV) only and verifies against any ciphertext produced under the same (key, IV) pair. The OpenSSL SSL/TLS implementation is not affected: AES-OCB is not a TLS cipher suite, and libssl does not call EVP_Cipher() in any case. Applications that drive AES-OCB through the documented streaming AEAD API (EVP_CipherUpdate / EVP_CipherFinal_ex) are not affected. Only applications that combine the AES-OCB cipher with the EVP_Cipher() one-shot API are vulnerable. The FIPS modules in 4.0, 3.6, 3.5, 3.4 and 3.0 are not affected by this issue, as AES-OCB is outside the OpenSSL FIPS module boundary.	7.5	More Details
CVE-	Issue summary: Receiving a QUIC initial packet with an invalid token may trigger a NULL pointer dereference in the OpenSSL QUIC server with address validation disabled. Impact summary: NULL pointer dereference typically causes abnormal termination of the affected QUIC server process and a Denial of Service. If the address validation is disabled in the OpenSSL QUIC server implementation, an attacker can		

2026-42764	crash the server by sending an initial packet with an invalid or expired token. By default, the client address validation is enabled in the OpenSSL QUIC server implementation, which makes the default configuration not vulnerable to this issue. However if the SSL_LISTENER_FLAG_NO_VALIDATE is used with the SSL_new_listener() call, the address validation is disabled making the vulnerable code reachable. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	7.5	More Details
CVE-2026-42765	Issue summary: When a partial-chain certificate verification is enabled together with OCSP response checking for the whole chain, a NULL dereference will happen if the verified chain does not have a self-signed trusted anchor, crashing the process. Impact summary: A NULL pointer dereference can trigger a crash which leads to a Denial of Service for an application. When performing OCSP response checking for certificates in the verification chain, the code always tries to access the next certificate as the issuer. There is a check for a self-signed certificate. However with the partial chain verification enabled when the chain does not have a self-signed trusted anchor, the issuer will be NULL for the last certificate in the chain. A NULL pointer dereference then happens. This issue affects only applications which enable both OCSP verification of the certificate chain (X509_V_FLAG_OCSP_RESP_CHECK_ALL) and partial chain verification (X509_V_FLAG_PARTIAL_CHAIN) in the certificate verification. Both flags are disabled by default. For that reason, we have assigned Low severity to the issue. No FIPS modules are affected by this issue as the affected code is outside the OpenSSL FIPS module boundary.	7.5	More Details
CVE-2026-41007	Spring HATEOAS maintains an unbounded static cache of StringLinkRelation instances keyed on attacker-supplied strings. Affected versions: Spring HATEOAS 1.5.0 through 1.5.6; 2.3.0 through 2.3.4; 2.4.0 through 2.4.1; 2.5.0 through 2.5.2; 3.0.0 through 3.0.3.	7.5	More Details
CVE-2026-36789	Shenzhen Tenda Technology Co., Ltd Tenda AC1206 v15.03.06.23 was discovered to contain multiple stack overflows in the fromGstDhcpSetSer function via the username and password parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-11694	Use after free in ServiceWorker in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-22164	Software installed and run as a non-privileged user may conduct improper GPU system calls to corrupt kernel heap memory. By creating resources of certain types and presenting a set of parameters to the affected interface the exploit can be used to corrupt kernel memory.	7.5	More Details
CVE-2026-11690	Out of bounds read and write in Media in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-41032	It is possible for an unauthenticated adjacent attacker to download log files of the controller, which may disclose some restricted information.	7.5	More Details
CVE-2026-34180	Issue summary: Parsing a crafted DER-encoded ASN.1 structure with a primitive element whose content exceeds 2 gigabytes in length may cause a heap buffer over-read on 64-bit Unix and Unix-like platforms. Impact summary: The heap buffer over-read may crash the application (Denial of Service) or to load into the decoded ASN.1 object contents of memory beyond the end of the input buffer. More typically such ASN.1 elements would instead be truncated. An integer truncation in OpenSSL's ASN.1 decoder causes the content length of an ASN.1 primitive element to be mishandled when it exceeds 2 gigabytes. In the worst case the truncated length is treated as a request to scan the binary content for a terminating zero byte, possibly causing OpenSSL to read either less than or beyond the end of the allocated buffer. Applications that pass attacker-supplied data to d2i_X509(), d2i_PKCS7(), or any other d2i_* decoding function are affected. OpenSSL's own command-line tools are not vulnerable, as data read through the BIO layer is checked before it reaches the affected code. The issue only affects 64-bit Unix and Unix-like platforms; 32-bit platforms and 64-bit Windows are not affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	7.5	More Details
CVE-2026-11242	Insufficient validation of untrusted input in Plugins in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-45291	Cloudburst Network provides network components used within Cloudburst projects. A vulnerability in versions prior to `1.0.0.CR3-20260418.124334-32` impacts publicly accessible software depending on the affected versions of Network and allows an attacker to exploit a bug in Network to close the parent netty channel, rendering it inoperable. All consumers of the library should upgrade to at least version `1.0.0.CR3-20260418.124334-32`. There are no known workarounds beyond updating the library.	7.5	More Details
CVE-	Shenzhen Tenda Technology Co., Ltd Tenda FH451 V1.0.0.9 was discovered to contain a stack overflow in		

2026-36785	the page parameter of the fromDhcpListClient function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-50234	Lyrion Music Server 9.2.0 contains a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting directory traversal in the web server context. Attackers can manipulate file path parameters to access sensitive files outside the intended directory structure.	7.5	More Details
CVE-2026-11255	Insufficient validation of untrusted input in Storage Access API in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-9516	Cpanel::JSON::XS versions before 4.41 for Perl allow denial of service via UTF-8 BOM prefixed input when a decode filter callback throws. To skip a leading 3-byte UTF-8 BOM, decode_json() advances the input scalar's string pointer past the mark with SvPV_set() and restores it only on the normal return path. When decoding aborts through a Perl exception, for example a filter_json_object callback that croaks, the restore is skipped and the scalar is left with its string pointer offset into its own buffer and a shortened length. When that scalar is later freed, the allocator receives an invalid pointer and the interpreter aborts. A single BOM prefixed document decoded with a throwing filter callback crashes any caller.	7.5	More Details
CVE-2026-40376	Improper input validation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2026-11239	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-45290	Cloudburst Network provides network components used within Cloudburst projects. A vulnerability in versions prior to `1.0.0.CR3-20260417.085727-30` impacts publicly accessible software depending on the affected versions of Network and allows an attacker to exploit a vulnerability in Network to stall the netty event loop, rendering it inoperable. All consumers of the library should upgrade to at least version `1.0.0.CR3-20260417.085727-30`. There are no known workarounds beyond updating the library.	7.5	More Details
CVE-2017-20250	Mac Photo Gallery 3.0 contains a path traversal vulnerability that allows unauthenticated attackers to download arbitrary files by manipulating the albid parameter. Attackers can send requests to macdownload.php with directory traversal sequences to access sensitive files like wp-load.php outside the intended plugin directory.	7.5	More Details
CVE-2026-9740	A vulnerability in MongoDB Server's BSON validation logic allows an unauthenticated user to crash the mongod process by sending a specially crafted message. The BSON validator's handling of certain nested binary data structures permits uncontrolled mutual recursion between validation functions, where each re-entry resets internal depth tracking.	7.5	More Details
CVE-2026-46493	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Versions prior to 26.0.1 use `uniqid` for generating salts, which is unsuitable. Version 26.0.1 fixes the issue.	7.5	More Details
CVE-2026-44799	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-42992	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-42993	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-50031	ipmi-oem in FreeIPMI before 1.6.18 has exploitable buffer overflows on response messages. The Intelligent Platform Management Interface (IPMI) specification defines a set of interfaces for platform management. It is implemented by a large number of hardware manufacturers to support system management. It is most commonly used for sensor reading (e.g., CPU temperatures through the ipmi-sensors command within FreeIPMI) and remote power control (the ipmipower command). The ipmi-oem client command implements a set of a IPMI OEM commands for specific hardware vendors. If a user has supported hardware, they may wish to use the ipmi-oem command to send a request to a server to retrieve specific information. Two subcommands "ipmi-oem dell get-active-directory-config" and "ipmi-oem fujitsu get-sel-entry-long-text" were found to have exploitable buffer overflows on response messages.	7.5	More Details

CVE-2026-40984	In Micrometer, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Affected versions: micrometer-core 1.16.0 through 1.16.5; 1.15.0 through 1.15.11; 1.14.0 through 1.14.15; 1.13.0 through 1.13.18; 1.9.0 through 1.9.17. micrometer-jetty11 1.16.0 through 1.16.5; 1.15.0 through 1.15.11; 1.14.0 through 1.14.15; 1.13.0 through 1.13.18. micrometer-jetty12 1.16.0 through 1.16.5; 1.15.0 through 1.15.11; 1.14.0 through 1.14.15; 1.13.0 through 1.13.18.	7.5	More Details
CVE-2026-46749	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected application uses a password hashing implementation with a static, hardcoded salt shared across all users and installations, and is configured with an insufficient number of iterations. This could allow an attacker to efficiently recover user passwords using brute-force or precomputed attacks, potentially resulting in unauthorized access.	7.5	More Details
CVE-2026-40983	In Micrometer, it is possible for a user to provide specially crafted gRPC requests that may cause a denial-of-service (DoS) condition. Affected versions: Micrometer 1.16.0 through 1.16.5; 1.15.0 through 1.15.11.	7.5	More Details
CVE-2026-42913	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-46374	SQLFluff is a modular SQL linter and auto-formatter with support for multiple dialects and templated code. Prior to version 4.2.0, in deployments where untrusted users can provide SQL queries to be linted, an untrusted user can submit a malicious long query to any application using the parser to trigger a Denial of Service through resource exhaustion. This issue has been patched in version 4.2.0.	7.5	More Details
CVE-2026-46373	SQLFluff is a modular SQL linter and auto-formatter with support for multiple dialects and templated code. Prior to version 4.1.0, in deployments where untrusted users can provide SQL queries to be linted, an untrusted user can submit a malicious query with deliberate excessive nesting to any application using the parser to trigger a Denial of Service through resource exhaustion. This issue has been patched in version 4.1.0.	7.5	More Details
CVE-2017-20248	Apptha Slider Gallery 1.0 contains a path traversal vulnerability that allows unauthenticated attackers to download arbitrary files by manipulating the imgname parameter. Attackers can send requests to asgallDownload.php with directory traversal sequences ../ to access sensitive files outside the intended directory.	7.5	More Details
CVE-2026-9742	When OIDC authentication is enabled in configuration, clients may set specific values in the "mechanism" parameter of the "authenticate" command that lead to server crash. The authenticate command is accessible to unauthenticated clients, leading to pre-auth denial-of-service in affected product configurations.	7.5	More Details
CVE-2026-41006	Spring HATEOAS's internal PropertyUtils.createObjectFromProperties method, used by the Collection+JSON and UBER media type deserializers, performs bean property binding via reflection without consulting Jackson access-control annotations. Affected versions: Spring HATEOAS 1.5.0 through 1.5.6; 2.3.0 through 2.3.4; 2.4.0 through 2.4.1; 2.5.0 through 2.5.2; 3.0.0 through 3.0.3.	7.5	More Details
CVE-2026-34713	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2026-11265	Inappropriate implementation in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	7.5	More Details
CVE-2026-9185	The 6Storage Rentals plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to and including 2.22.0 via the `userId` parameter of the `six_storage_get_user_info` and `six_storage_update_profile` AJAX actions. This is due to the `six_storage_getUserInfo()` and `six_storage_updateProfile()` functions being registered on `wp_ajax_nopriv_*` hooks and accepting a tenant identifier directly from `$_POST['userId']` without performing any ownership verification, session binding, or nonce validation to confirm the requester has a legitimate relationship to the supplied ID. This makes it possible for unauthenticated attackers to read and modify arbitrary tenants' profile data — including name, email address, phone number, physical address, and SSN — by supplying an enumerated `userId` value in a crafted request to either handler.	7.5	More Details
CVE-2026-11641	Use after free in Bluetooth in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	7.5	More Details
CVE-2026-	Use after free in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	7.5	More

11154	(Chromium security severity: Medium)		Details
CVE-2026-10899	Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.53 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: Critical)	7.5	More Details
CVE-2026-39169	SEMCMS 5.0 is vulnerable to unauthorized access in SEMCMS_copy.php.	7.5	More Details
CVE-2026-49847	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, a single unauthenticated WebSocket frame containing a deeply nested JSON document crashes the FreeSWITCH process via stack overflow, terminating all calls and sessions on the host. The recursion drives the worker thread's stack pointer into the stack guard page, raising SIGSEGV from the kernel before any usable write primitive develops. This issue has been patched in version 1.11.1.	7.5	More Details
CVE-2026-10900	Use after free in Passwords in Google Chrome on Mac prior to 149.0.7827.53 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: Critical)	7.5	More Details
CVE-2026-49975	Memory Allocation with Excessive Size Value vulnerability in Apache HTTP Server's mod_http leads to denial of service via malicious HTTP requests. This issue affects Apache HTTP Server: from 2.4.17 through 2.4.67.	7.5	More Details
CVE-2026-10901	Use after free in Passwords in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	7.5	More Details
CVE-2025-55657	A NULL pointer dereference in the gf_odf_vvc_cfg_write_bs function (odf/descriptors.c) of GPAC MP4Box v2.4 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MP4 file.	7.5	More Details
CVE-2026-49494	Comodo Internet Security's firewall driver Inspect.sys contains an integer underflow in its IPv6 packet parser. The parser decrements an unsigned 64-bit payload-length value (taken from the IPv6 fixed header's payload length field) by the size of each IPv6 extension header without validating it, so a packet whose declared payload length is smaller than the sum of its extension-header lengths underflows the value to a near-maximal 64-bit integer. Because IPv6 parsing occurs before firewall rule enforcement, a remote, unauthenticated attacker can send a single crafted IPv6 packet - even to a host with all ports blocked - to trigger an out-of-bounds read (and, on a separate code path, an oversized memcpy) in the Windows kernel at DISPATCH_LEVEL, crashing the system (BSOD).	7.5	More Details
CVE-2026-10796	nvm (Node Version Manager) through 0.40.4 executes arbitrary commands from version strings supplied by the configured Node.js/io.js mirror. Commands such as `nvm install` read the available versions from the mirror's index.tab and use the selected version, without sanitization, to build download URLs and shell/awk commands. Two sinks are affected by the same untrusted input: nvm_download() built a curl/wget command string and ran it with `eval`, so a version field containing command substitution (for example $(id)) was executed by the local shell; and nvm_get_checksum() interpolated the version-derived download slug into an awk program, so a crafted version could execute arbitrary commands via awk's system(). An attacker who controls the configured mirror, supplies mirror content to a user or CI on a non-default mirror, or machine-in-the-middles a non-TLS mirror can ∴ run arbitrary commands with the privileges of the user running nvm. The default mirror (https://nodejs.org over TLS) is not affected. Fixed on master (pending the next tagged release) by passing every argument as a literal argv element instead of using eval, by passing the value to awk as data via -v instead of interpolating it into the program, and by rejecting any version outside the Node.js/io.js version grammar before it is used.	7.5	More Details
CVE-2026-11151	Insufficient validation of untrusted input in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-49193	Overly permissive configuration settings on cloud storage containers expose active telemetry information publicly to the internet.	7.5	More Details
CVE-2026-49160	Uncontrolled resource consumption in HTTP/2 allows an unauthorized attacker to deny service over a network.	7.5	More Details
	Net::CIDR::Set versions through 0.20 for Perl did not validate IP addresses. The add method called the		

CVE-2026-49941	_encode method to parse addresses. If the addresses did not look like netmasks or network ranges, then they were assumed to single IP addresses and passed back to itself as a 32-bit or 128-bit netmask. If the argument was not a well-formed IP address, then this would lead to indefinite recursion. An attacker could use this to cause a denial of service.	7.5	More Details
CVE-2026-8878	Version 3.0.7 of the Securly Chrome Extension exposes multiple publicly accessible endpoints that allow unauthenticated access to sensitive data. The exposed information consists of SHA-1 hashes that are inadequately obfuscated using a simple Caesar cipher, which can be easily reversed to recover the original hash values and access the protected data.	7.5	More Details
CVE-2026-36771	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain a stack overflow in the wl_radio parameter of the formwrlSSIDset function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-11632	Use after free in TabStrip in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	7.5	More Details
CVE-2026-49475	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.0, a STUN packet whose declared attribute length is shorter than the structure the parser casts to causes the parser to read and write past the end of the attribute, producing an out-of-bounds memory access on the per-leg media buffer. This issue has been patched in version 1.11.0.	7.5	More Details
CVE-2026-36823	Shenzhen Tenda Technology Co., Ltd Tenda W20E v15.11.0.6 was discovered to contain a buffer overflow in the webAuthUserInfo parameter of the formAddWebAuthUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-45639	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-36770	Shenzhen Tenda Technology Co., Ltd Tenda US_W3V1.0BR v1.0.0.3 was discovered to contain a stack overflow in the Go parameter of the ask_to_reboot function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-10737	The SP Project & Document Manager plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the view_file function in all versions up to, and including, 4.71. This makes it possible for unauthenticated attackers to read file metadata and obtain download links for arbitrary files stored inside project folders on the server, which can contain sensitive information. The authorization gate uses a negated nonce check OR-chained with permission checks, meaning a missing or invalid nonce causes the entire condition to evaluate to true and bypass all preceding capability and ownership checks. The secondary fallback check only denies access for root-level files (pid == 0), leaving all files stored inside project folders fully exposed to unauthenticated users who supply only a valid file ID in a POST request to admin-ajax.php.	7.5	More Details
CVE-2026-10969	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-49842	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, mod_verto's WebSocket frame loop intercepts a #-prefixed speed-test protocol (#SPU / #SPB / #SPE) before any authentication check. The declared payload size in #SPU was parsed with atoi() and only rejected non-positive values, so an unauthenticated peer could request up to INT_MAX bytes. The server then wrote roughly size * 10 bytes back during the download phase, on the order of 20 GB per request, yielding strong outbound bandwidth amplification from a short request. This issue has been patched in version 1.11.1.	7.5	More Details
CVE-2026-36819	Shenzhen Tenda Technology Co., Ltd Tenda W20E v15.11.0.6 was discovered to contain a buffer overflow in the bindMACAddr parameter of the fromSetDhcpRules function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-41858	Weak Randomness / Insecure Cryptographic Primitive (CWE-338) in Get-RandomPassword in BOSH-Ecosystem / windows-utilities-release allows a network attacker to estimate VM boot time and reconstruct a small candidate list to recover the Administrator password. The randomize_password job exists solely to lock the local Administrator account behind an unguessable password as a hardening control. Because the password is derived from a predictable, clock-seeded PRNG, a network attacker who can estimate VM boot time can reconstruct a small candidate list and recover the Administrator password, defeating the hardening control. Affected versions: - windows-utilities-release: all versions prior to v0.23.0 (inclusive); fixed in v0.23.0 or later	7.5	More Details

CVE-2023-54350	WordPress Augmented-Reality plugin contains a remote code execution vulnerability in the elFinder connector that allows unauthenticated attackers to upload and execute arbitrary PHP files. Attackers can send POST requests to the connector.minimal.php endpoint with mkfile and put commands to create malicious PHP files in the file_manager directory and execute them on the server.	7.5	More Details
CVE-2026-8829	HTML::Entities versions before 3.84 for Perl read freed heap memory in _decode_entities. The XS routine backing HTML::Entities::_decode_entities cached a pointer (repl) into the entity-value SV returned by hv_fetch on the entity2char hash. When the input SV was identical to a value SV in that hash, and that value contained its own key as an entity reference, a later call to grow_gap() reallocated the SV's PV buffer and freed the backing allocation that repl still pointed into. The subsequent copy loop read repl_len bytes from the freed allocation. The read may disclose adjacent heap contents into the destination SV.	7.5	More Details
CVE-2026-36820	Shenzhen Tenda Technology Co., Ltd Tenda W20E v15.11.0.6 was discovered to contain a buffer overflow in the webAuthWhiteUserInfo parameter of the formAddWebAuthWhiteUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-46265	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix WQ_MEM_RECLAIM warning When sunrpc is used, if a reset triggered, our wq may lead the following trace: workqueue: WQ_MEM_RECLAIM xprtiod:xprt_rdma_connect_worker [rpcrdma] is flushing !WQ_MEM_RECLAIM hns_roce_irq_workq:flush_work_handle [hns_roce_hw_v2] WARNING: CPU: 0 PID: 8250 at kernel/workqueue.c:2644 check_flush_dependency+0xe0/0x144 Call trace: check_flush_dependency+0xe0/0x144 start_flush_work.constprop.0+0x1d0/0x2f0 __flush_work.isra.0+0x40/0xb0 flush_work+0x14/0x30 hns_roce_v2_destroy_qp+0xac/0x1e0 [hns_roce_hw_v2] ib_destroy_qp_user+0x9c/0x2b4 rdma_destroy_qp+0x34/0xb0 rpcrdma_ep_destroy+0x28/0xcc [rpcrdma] rpcrdma_ep_put+0x74/0xb4 [rpcrdma] rpcrdma_xprt_disconnect+0x1d8/0x260 [rpcrdma] xprt_rdma_connect_worker+0xc0/0x120 [rpcrdma] process_one_work+0x1cc/0x4d0 worker_thread+0x154/0x414 kthread+0x104/0x144 ret_from_fork+0x10/0x18 Since QP destruction frees memory, this wq should have the WQ_MEM_RECLAIM.	7.5	More Details
CVE-2026-36821	Shenzhen Tenda Technology Co., Ltd Tenda W20E v15.11.0.6 was discovered to contain a buffer overflow in the picCropName parameter of the formCropAndSetWewifiPic function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-36822	Shenzhen Tenda Technology Co., Ltd Tenda W20E v15.11.0.6 was discovered to contain a buffer overflow in the macAddr parameter of the formDelStaState function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2025-8873	On affected platforms running Arista EOS with IPsec configured, a specially crafted packet can cause the dataplane to stop processing all IPsec traffic. The control plane may detect this condition, and attempt to reset the IPsec processing pipeline. After reset traffic may not resume being processed. There is no impact to non-IPsec traffic or to IPsec traffic not originating or terminating on the system. This issue was reported by an Arista customer.	7.5	More Details
CVE-2026-45583	Improper control of generation of code ('code injection') in Microsoft Exchange Server allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-45591	Uncontrolled resource consumption in ASP.NET Core allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-40519	Nginx Proxy Manager versions 2.9.14 through 2.15.1, fixed in commit a5db5ed, contain an authenticated remote code execution vulnerability via OS command injection in the setupCertbotPlugins() function in backend/setup.js, allowing attackers with certificates:manage permission to execute arbitrary commands by storing a malicious payload in the dns_provider_credentials field. The user-controlled dns_provider_credentials value is interpolated directly into a shell command executed via child_process.exec() without sanitization or escaping, causing the injected command to execute upon backend restart.	7.5	More Details
CVE-2026-46741	Etsy::StatsD versions through 1.002002 for Perl allow metric injections. The metric names and values are not checked for newlines, colons or pipes. Metrics generated from untrusted sources could inject additional statsd metrics. Note that the git repository contains an unreleased version with the gauge and set methods that also do not check for potential metric injections.	7.5	More Details
CVE-2026-	Version 3.0.7 of the Securly Chrome Extension dynamically registers content13.min.js as a content script via chrome.scripting.registerContentScripts() at runtime. This script is NOT declared in manifest.json and bypasses Chrome Web Store static security review. It runs on all URLs and immediately hides all page	7.5	More Details

8879	content, creates a full-page overlay, pauses all videos, and only restores content when the service worker confirms the page passes filtering. If Securly's servers are unreachable, pages remain indefinitely hidden.		
CVE-2026-3238	A flaw was found in Samba’s WINS server component when running as an Active Directory Domain Controller. The WINS protocol handlers for certain request types did not properly validate incoming packets, allowing an unauthenticated remote attacker to trigger a NULL pointer dereference and crash the WINS service using specially crafted UDP packets.	7.5	More Details
CVE-2026-10725	Protocol::HTTP2 versions before 1.13 for Perl is vulnerable to a HTTP/2 Bomb. Protocol::HTTP2's inbound HPACK path has no header-list size limit, so a small HTTP/2 request can expand into large server memory (the "HTTP/2 bomb"). The headers_decode method materialises a full key+value copy per indexed reference with no running size check, and the stream_header_block_add method appends (since version 1.12) every CONTINUATION frame to the per-stream buffer unbounded. MAX_HEADER_LIST_SIZE (default 65536) is advertised in SETTINGS but never consulted on decode. It is absent from the decoder and from the :limits export tag.	7.5	More Details
CVE-2026-47654	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-10946	Heap buffer overflow in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-34356	Heap-based Buffer Overflow vulnerability in Apache HTTP Server with malicious backend servers and ProxyPassReverseCookie* This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	7.5	More Details
CVE-2026-45771	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.0, FreeSWITCH's bundled XML parser expands nested <!ENTITY> declarations without a depth or count bound, so a small DTD can describe a body that expands exponentially ("billion laughs"). The PIDF body of a SIP PUBLISH is fed to this parser before any digest check, letting an unauthenticated network attacker force unbounded CPU and memory consumption with a single request. This issue has been patched in version 1.11.0.	7.5	More Details
CVE-2026-34355	A buffer overflow in mod_proxy_html in Apache HTTP Server 2.4.67 and earlier allows an attack by an untrusted backend. Users are recommended to upgrade to version 2.4.68, which fixes this issue.	7.5	More Details
CVE-2026-50210	The device encrypts data using AES-CBC with static zero-filled Initialization Vectors (IVs), making it susceptible to replay attacks and known-plaintext decryption.	7.5	More Details
CVE-2026-8888	Version 3.0.7 of the Securly Chrome Extension downloads config.json over HTTP and compiles server-provided patterns as JavaScript regular expressions via new RegExp() without complexity validation. An on-path attacker can inject specific patterns to cause catastrophic backtracking, resulting in denial of service on all browsing.	7.5	More Details
CVE-2026-8889	Version 3.0.7 of the Securly Chrome Extension uses deprecated SHA-1 hashing for IWF CSAM URL matching (25,020 hashes) and CIPA blocklist matching (12,352 hashes).	7.5	More Details
CVE-2025-52293	A segmentation violaton in the gf_hevc_read_sps_bs_internal function (media_tools/av_parsers.c) of GPAC MP4Box v2.4 allows attackers to cause a Denial of Service (DoS) via supplying crafted HEVC SPS data.	7.5	More Details
CVE-2026-28318	SolarWinds Serv-U is susceptible to specially crafted POST requests that crash the Serv-U service without authentication using Content-Encoding: deflate. Mitigation steps are provided to secure customer environments in the SolarWinds Trust Center if you are unable to deploy the update	7.5	More Details
CVE-2026-37462	An integer underflow in the BGPUpdate.DecodeFromBytes function (/bgp/bgp.go) of gobgp v4.3.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted BGP UPDATE message.	7.5	More Details
CVE-2026-10906	Use after free in WebAuthentication in Google Chrome prior to 149.0.7827.53 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: High)	7.5	More Details
CVE-2025-	A stack buffer overflow in the filein_process function (in_file.c) of GPAC MP4Box v2.4 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MP4 file.	7.5	More Details

52292			
CVE-2023-43688	An issue was discovered in Malwarebytes 4.x and 5.x (and Nebula 2020-10-21 and later). There is a Heap buffer overflow in various buffer encryption utilities.	7.5	More Details
CVE-2026-9290	The WP User Manager – User Profile Builder & Membership plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.9.17 via the (profile template scope) function. This makes it possible for unauthenticated attackers to include and execute arbitrary .php 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 .php file types can be uploaded and included.	7.5	More Details
CVE-2026-36786	Shenzhen Tenda Technology Co., Ltd Tenda FH451 V1.0.0.9 was discovered to contain a stack overflow in the list1 parameter of the fromDhcpListClient function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2026-8881	Version 3.0.7 of the Securly Chrome Extension uses EVP_BytesToKey key derivation with MD5 and a single iteration for AES encryption. MD5 has been broken since 2004 and a single iteration provides no key stretching.	7.5	More Details
CVE-2026-42536	Heap-based Buffer Overflow vulnerability in Apache HTTP Server with mod_xml2enc, xml2StartParse, and untrusted content This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	7.5	More Details
CVE-2026-49187	The hard-coded APK resource files never expire, and the shared scepter leads to information leaks and potential misuse.	7.5	More Details
CVE-2026-11636	Use after free in Autofill in Google Chrome on Windows prior to 149.0.7827.103 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: Critical)	7.5	More Details
CVE-2026-11639	Use after free in Compositing in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	7.5	More Details
CVE-2025-46638	Dell BSAFE SSL-J contains an allocation of resources without limits or throttling vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to a Denial of Service (DoS).	7.5	More Details
CVE-2026-38570	bacnet_stack 1.3.1 contains an Out-of-bounds Read in bacnet_tag_number_decode which allows attackers to cause a denial of service.	7.5	More Details
CVE-2026-9076	Issue summary: When CMS password-based decryption (RFC 3211 / PWRI key unwrap) processes attacker-supplied CMS data, an attacker-chosen stream-mode KEK cipher can trigger a heap out-of-bounds read in kek_unwrap_key(). Impact summary: A heap buffer over-read may trigger a crash which leads to Denial of Service for an application if the input buffer ends at a memory page boundary and the following page is unmapped. There is no information disclosure as the over-read bytes are not revealed to the attacker. The key unwrapping function performs a check-byte test as specified in the RFC that reads 7 bytes from a heap allocation that is based on the wrapped key length from the message. There is a minimum length check based on the block length of the wrapping cipher. However the cipher is selected from an OID carried in the attacker's PWRI keyEncryptionAlgorithm with no requirement that the cipher be a block cipher. When an attacker selects a stream-mode cipher the guard will be ineffective and the allocated buffer containing the unwrapped key can be too small to fit the check-bytes specified in the RFC and a buffer over-read can happen. Applications calling CMS_decrypt() or CMS_decrypt_set1_password() (equivalently openssl cms -decrypt -pwri_password ...) on untrusted CMS data are vulnerable to this issue. No password knowledge is required: the over-read happens during the unwrap attempt before any authentication succeeds. The over-read is limited to a few bytes and is not written to output, so there is no information disclosure. Triggering a crash requires the allocation to border unmapped memory, which is unlikely with the normal allocator. The FIPS modules are not affected by this issue.	7.5	More Details
CVE-2026-11058	Integer overflow in CredentialProvider in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform OS-level privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-11667	Out of bounds read in WebRTC in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the GPU process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details

CVE-2026-48563	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	7.5	More Details
CVE-2026-11149	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2026-11644	Use after free in Views in Google Chrome on Linux prior to 149.0.7827.103 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Critical)	7.5	More Details
CVE-2026-50213	The account validation endpoint /v1/User/validate returns comprehensive user profile data sheets, which can be crawled by iterating predictable identification strings.	7.5	More Details
CVE-2025-71319	image-size 1.1.0 before 1.2.1 and 2.0.0 before 2.0.2 contain a denial of service vulnerability in the findBox function when processing specially crafted images with zero-sized boxes. Remote attackers can cause application hang by supplying malicious JXL, HEIF, or JP2 image files with box size zero, triggering infinite loops during image validation.	7.5	More Details
CVE-2026-10968	Insufficient validation of untrusted input in Dawn in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	7.4	More Details
CVE-2026-10976	Uninitialized Use in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	7.4	More Details
CVE-2026-47960	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	7.4	More Details
CVE-2026-10973	Uninitialized Use in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	7.4	More Details
CVE-2026-47937	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	7.4	More Details
CVE-2026-44393	An issue was discovered in OpenStack oslo.messaging 1.0.0 through 17.3.0. The oslo.messaging RabbitMQ driver does not perform TLS hostname verification when connecting to the message broker. When ssl_ca_file is configured, the driver enables certificate chain validation but does not pass the expected broker hostname into the underlying TLS stack. Any certificate signed by the deployment CA is accepted regardless of hostname, allowing an attacker who can intercept control-plane traffic to impersonate the RabbitMQ broker and perform a man-in-the-middle attack on RPC and notification traffic. All OpenStack services using oslo.messaging with RabbitMQ over TLS are affected.	7.4	More Details
CVE-2025-14774	Incorrect Authorization vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	7.4	More Details
CVE-2026-45300	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Versions on the 2.x branch prior to 2.15.0 and the 3.x branch prior to 3.0.10 leak `Cookie` headers to cross-origin redirect targets. When following a redirect to a different origin, the `propagatedHeaders()` method in `Redirect30xInterceptor.java` strips `Authorization` and `Proxy-Authorization` headers but does not strip the `Cookie` header, causing session cookies and other sensitive cookie values to be sent to attacker-controlled servers. Versions 2.15.0 and 3.0.10 patch the issue.	7.4	More Details
CVE-2026-50292	In libinput before 1.30.4 and 1.31.x before 1.31.3, libinput-device-group unescaped phys output can inject udev properties leading to arbitrary root code execution	7.4	More Details
CVE-2026-	A weakness in the certificate validation logic of the deprecated IKEv1 key exchange may allow an unauthenticated attacker positioned as a man-in-the-middle to bypass certificate validation in VPN site-to-site connections that use certificate-based authentication. Successful exploitation could allow	7.4	More Details

50752	interception or modification of traffic traversing the VPN tunnel.		
CVE-2026-41720	Spring LDAP's DirContextAuthenticationStrategy implementations do not reject a bind request where a non-empty username is paired with an empty or null password. Affected versions: Spring LDAP 2.4.0 through 2.4.4; 3.2.0 through 3.2.17; 3.3.0 through 3.3.7; 4.0.0 through 4.0.3.	7.4	More Details
CVE-2026-10777	A vulnerability was identified in ealpha072 Student-Management-System up to 01451bd7a2f58cdda07bd0b86e3967582e3ecd08. Affected by this issue is some unknown functionality of the file admin/config.php of the component Administrative Backend. Such manipulation leads to improper authentication. The attack may be performed from remote. The exploit is publicly available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-11485	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /archive2.php. Such manipulation of the argument sy leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-11482	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is an unknown function of the file /archive5.php. The manipulation of the argument sy leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-11483	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0. This affects an unknown function of the file /archive4.php. The manipulation of the argument sy results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-11489	A vulnerability was found in code-projects Online Music Site 1.0. This vulnerability affects unknown code of the file /Administrator/PHP/AdminDeleteAlbum.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-47634	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	7.3	More Details
CVE-2026-11488	A vulnerability has been found in code-projects Simple Flight Ticket Booking System 1.0. This affects an unknown part of the file checkUser.php of the component POST Parameter Handler. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-24180	NVIDIA DALI contains a vulnerability in a component where an attacker could cause a heap-based buffer overflow. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	7.3	More Details
CVE-2026-24181	NVIDIA DALI contains a vulnerability in a component where an attacker could cause an improper index validation. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	7.3	More Details
CVE-2026-9334	Cpanel::JSON::XS versions before 4.41 for Perl allow type confusion via duplicate object keys when dupkeys_as_arrayref is enabled. decode_hv() collapses duplicate object keys into an array reference under dupkeys_as_arrayref. The branch reached for a duplicate key tests `SvTYPE (old_value) != SVt_RV && SvTYPE (SvRV (old_value)) != SVt_PVAV`, which evaluates SvRV(old_value) before establishing that old_value is a reference. When the existing value is a plain scalar rather than an array reference, a non-reference scalar is dereferenced as a reference. A caller decoding untrusted JSON with dupkeys_as_arrayref enabled is crashed, and the incompatible access follows a pointer taken from attacker controlled scalar contents.	7.3	More Details
CVE-2026-50593	Graphite before 1.3.15 has an integer underflow and resultant out-of-bounds write via Graphite actions, because slotat does not ensure that an offset is within the allowed slot-map range.	7.3	More Details
CVE-2026-11490	A vulnerability was determined in code-projects Online Music Site 1.0. This issue affects some unknown processing of the file /Frontend/Search.php. This manipulation of the argument Category causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-	A vulnerability was detected in SourceCodester Pizzafy E-Commerce System 1.0. Affected by this vulnerability is the function Login of the file /admin/admin_class_novo.php of the component		More

2026-10704	Administrative Control Panel. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	Details
CVE-2026-11486	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /archive1.php. Performing a manipulation of the argument sy results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	7.3	More Details
CVE-2026-49942	Net::CIDR::Set versions through 0.20 for Perl did not validate network masks. The mask portion of a network mask could contain Unicode digits such as the Arabic-Indic One (U+0661), or non-digits, which were ignored. This could allow network masks to accept larger networks. Leading zeros were also accepted, but treated as decimal instead of octal. This could lead to confusion about what networks are acceptable.	7.3	More Details
CVE-2026-11531	A security flaw has been discovered in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. This impacts an unknown function of the file admin/admin_login.php of the component Administrator Login Endpoint. Performing a manipulation of the argument a_usr/a_pwd results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-11530	A vulnerability was identified in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. This affects an unknown function of the file /index.ph of the component Login. Such manipulation of the argument usr/pwd leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-10771	A vulnerability was found in crmeb crmeb_java 1.4. Affected is the function RestTemplate.getForEntity of the file crmeb-common/src/main/java/com/zbkj/common/utils/RestTemplateUtil.java of the component base64 Qrcode Endpoint. The manipulation of the argument url results in server-side request forgery. The attack can be executed remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-11344	A vulnerability was found in code-projects Vehicle Management System 1.0. This impacts an unknown function of the file newdriver.php of the component New Driver Registration Form. Performing a manipulation of the argument photo results in unrestricted upload. The attack may be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-11484	A weakness has been identified in SourceCodester Class and Exam Timetabling System 1.0. This impacts an unknown function of the file /archive3.php. This manipulation of the argument sy causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-11342	A vulnerability has been found in code-projects Hotel and Tourism Reservation System 1.0. This affects an unknown function of the file /details.php. Such manipulation of the argument room leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-48913	Use After Free vulnerability in Apache HTTP Server module mod_http2 when file handles are already exhausted. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.67.	7.3	More Details
CVE-2026-11501	A security flaw has been discovered in SourceCodester Hospitals Patient Records Management System 1.0. This issue affects some unknown processing of the file /classes/Master.php?f=save_patient. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-11462	A vulnerability was found in Chengdu Everbrite Network Technology BeikeShop up to 1.6.0.22. This impacts the function callback of the file plugins/Stripe/Controllers/StripeController.php of the component Stripe Plugin. Performing a manipulation of the argument Request results in improper authorization. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named 6719e0fc690ea0a998452092862e0f0a17c65968. It is suggested to install a patch to address this issue.	7.3	More Details
CVE-2026-	A vulnerability was identified in Chanjet CRM 1.0. This affects an unknown part of the file /tools/jxf_dump_systable.php of the component HTTP GET Request Handler. Such manipulation of the argument gblOrgID leads to sql injection. The attack may be launched remotely. The exploit is publicly	7.3	More

11456	available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2026-11618	A vulnerability was determined in DTStack Taier up to 1.4.0. The affected element is the function preHandle of the file taier-data-develop/src/main/java/com/dtstack/taier/develop/interceptor/LoginInterceptor.java of the component Source Connection Test Endpoint. Executing a manipulation can lead to improper authentication. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This patch is called f95389e7f74acec42bcee079a616aaa06f9551d2. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2026-11463	A vulnerability was determined in USCiLab Cereal up to 1.3.2. Affected is an unknown function of the component Shared Pointer Handler. Executing a manipulation can lead to type confusion. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	7.3	More Details
CVE-2026-36609	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 uses a static authentication nonce that does not change between requests from the same source IP. Combined with the predictable XOR-based password encoding (securityEncode function), this allows an attacker to reverse captured authentication tokens to recover the plaintext password.	7.3	More Details
CVE-2026-11460	A flaw has been found in Boost Serialization up to 1.91. The impacted element is an unknown function. This manipulation causes improper validation of specified type of input. It is possible to initiate the attack remotely. The exploit has been published and may be used. The maintainer was notified on Aug 2025 and a disclosure deadline was set for 90 days. The maintainer acknowledged but postponed indefinitely citing time concerns. No patch is currently available and the disclosure deadline has expired.	7.3	More Details
CVE-2026-11115	Use after free in Updater in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	7.3	More Details
CVE-2026-11334	A vulnerability was detected in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. This affects an unknown function of the file dashboard_page/forms/fetch.php. Performing a manipulation of the argument department_code results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of 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-2026-11457	A security flaw has been discovered in erzhongxmu JeeWMS up to 141740afb2ba14d441c82a833d0a418d07ca2d69. This vulnerability affects unknown code of the file /base-boot/jmreport/testConnection of the component JimuReport test-connection Endpoint. Performing a manipulation of the argument dbType/dbDriver/dbUrl/dbUsername/dbPassword results in injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-11452	A vulnerability has been found in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function FUN_0042e200 of the file /cgi-bin/glc of the component SET_USER_PWD Handler. The manipulation of the argument Password leads to command injection. The attack can be initiated remotely. Upgrading to version 4.8.1 is able to address this issue. The affected component should be upgraded. The vendor explains: " The current code escapes single quotes in the password parameter and handles it inside a shell single-quote context. The payloads in the report, which rely on $() or backticks to trigger command substitution, are not executed under the current code path. We tested on a GL-MT3000 device running firmware 4.8.1 using similar payloads, and no command-execution marker file was created."	7.3	More Details
CVE-2026-11471	A vulnerability was found in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is an unknown function of the file /index2.php. The manipulation of the argument Password results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-11451	A flaw has been found in GL.iNet GL-MT3000 4.4.5. This impacts the function snprintf of the file /cgi-bin/glc of the component FTP Protocol Handler. Executing a manipulation of the argument media_dir can lead to command injection. It is possible to launch the attack remotely. Upgrading to version 4.8.1 will fix this issue. You should upgrade the affected component. The vendor explains: "In version 4.8.1, before writing media_dir to the FTP configuration command, the code escapes single quotes using escape_single_quote(). The payloads in the report—which rely on closing a single quote, appending commands with a semicolon, and commenting out the tail with #—cannot escape execution under the current code path. We also verified this on a GL-MT3000 device running firmware version 4.8.1 using	7.3	More Details

	similar payloads calling the /NAS_API_SET_PROTO_CONFIG interface. Although the interface returned success, the marker file intended to prove command execution was not created; the payload was written into /etc/vsftpd.conf only as ordinary configuration content and did not trigger any shell command execution. Therefore, with the current firmware version and default runtime environment, we could not reproduce the claimed “unauthorized command injection in set_proto_config”."		
CVE-2026-11450	A vulnerability was detected in GL.iNet GL-MT3000 4.4.5. This affects the function dlopen in the library /usr/lib/oui-httpd/rpc/ of the component Path Normalization Handler. Performing a manipulation of the argument dev_name results in command injection. It is possible to initiate the attack remotely. Upgrading to version 4.7 mitigates this issue. It is advisable to upgrade the affected component. The vendor confirms: " From version 4.7 onward, we have enabled method-level validation at the HTTP /rpc layer. nas-web.eject_disk is no longer in the whitelist of allowed methods. Consequently, directly calling eject_disk through the default /rpc endpoint returns Invalid params, preventing entry into subsequent dangerous functions and blocking the remote exploit chain described in the report."	7.3	More Details
CVE-2026-45481	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	7.3	More Details
CVE-2026-46250	In the Linux kernel, the following vulnerability has been resolved: MIPS: Work around LLVM bug when gp is used as global register variable On MIPS, __current_thread_info is defined as global register variable locating in $gp, and is simply assigned with new address during kernel relocation. This however is broken with LLVM, which always restores $gp if it finds $gp is clobbered in any form, including when intentionally through a global register variable. This is against GCC's documentation[1], which requires a callee-saved register used as global register variable not to be restored if it's clobbered. As a result, $gp will continue to point to the unrelocated kernel after the epilog of relocate_kernel(), leading to an early crash in init_idle, [0.000000] CPU 0 Unable to handle kernel paging request at virtual address 0000000000000000, epc == ffffffff81afada8, ra == ffffffff81afad90 [0.000000] Oops[#1]: [0.000000] CPU: 0 UID: 0 PID: 0 Comm: swapper Tainted: G W 6.19.0-rc5-00262-gd3eeb99bbc99-dirty #188 VOLUNTARY [0.000000] Tainted: [W]=WARN [0.000000] Hardware name: loongson,loongson64v-4core-virtio [0.000000] $ 0 : 0000000000000000 0000000000000000 0000000000000001 0000000000000000 [0.000000] $ 4 : ffffffff80b80ec0 ffffffff80b53d48 0000000000000000 00000000000f4240 [0.000000] $ 8 : 0000000000000100 ffffffff81d82f80 ffffffff81d82f80 0000000000000001 [0.000000] $12 : 0000000000000000 ffffffff81776f58 00000000000005da 0000000000000002 [0.000000] $16 : ffffffff80b80e40 0000000000000000 ffffffff80b81614 9800000005dfbe80 [0.000000] $20 : 00000000540000e0 ffffffff81980000 0000000000000000 ffffffff80f81c80 [0.000000] $24 : 0000000000000a26 ffffffff8114fb90 [0.000000] $28 : ffffffff80b50000 ffffffff80b53d40 0000000000000000 ffffffff81afad90 [0.000000] Hi : 0000000000000000 [0.000000] Lo : 0000000000000000 [0.000000] epc : ffffffff81afada8 init_idle+0x130/0x270 [0.000000] ra : ffffffff81afad90 init_idle+0x118/0x270 [0.000000] Status: 540000e2 KX SX UX KERNEL EXL [0.000000] Cause : 00000008 (ExcCode 02) [0.000000] BadVA : 0000000000000000 [0.000000] PrId : 00006305 (ICT Loongson-3) [0.000000] Process swapper (pid: 0, threadinfo=(____ptrval____), task=(____ptrval____), tls=0000000000000000) [0.000000] Stack : 9800000005dfbf00 ffffffff8178e950 0000000000000000 0000000000000000 [0.000000] 0000000000000000 ffffffff81970000 000000000000003f ffffffff810a6528 [0.000000] 0000000000000001 9800000005dfbe80 9800000005dfbf00 ffffffff81980000 [0.000000] ffffffff810a6450 ffffffff81afb6c0 0000000000000000 ffffffff810a2258 [0.000000] ffffffff81d82ec8 ffffffff8198d010 ffffffff81b67e80 ffffffff8197dd98 [0.000000] ffffffff81d81c80 ffffffff81930000 0000000000000040 0000000000000000 [0.000000] 0000000000000000 0000000000000000 0000000000000000 0000000000000000 [0.000000] 0000000000000000 000000000000009e ffffffff9fc01000 0000000000000000 [0.000000] 0000000000000000 0000000000000000 0000000000000000 0000000000000000 [0.000000] 0000000000000000 ffffffff81ae86dc ffffffff81b3c741 0000000000000002 [0.000000] ... [0.000000] Call Trace: [0.000000] [<ffffffff81afada8>] init_idle+0x130/0x270 [0.000000] [<ffffffff81afb6c0>] sched_init+0x5c8/0x6c0 [0.000000] [<ffffffff81ae86dc>] start_kernel+0x27c/0x7a8 This bug has been reported to LLVM[2] and affects version from (at least) 18 to 21. Let's work around this by using inline assembly to assign $gp before a fix is widely available.	7.3	More Details
CVE-2026-11035	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to perform privilege escalation via a crafted XML file. (Chromium security severity: Medium)	7.3	More Details
CVE-2026-11437	A flaw has been found in perfree go-fastdfs-web up to 1.3.7. Affected is the function checkServer of the file /install/checkServer of the component Installation Endpoint. Executing a manipulation can lead to server-side request forgery. The attack can be executed 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-2026-11435	A security vulnerability has been detected in Jinher OA 1.0. This affects an unknown function of the file nextselectplan.aspx. Such manipulation of the argument httpOID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted	7.3	More Details

	early about this disclosure but did not respond in any way.		
CVE-2026-11582	A flaw has been found in CodeAstro Student Attendance Management System 1.0. The impacted element is an unknown function of the file /attendance-php/index.php. Executing a manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	7.3	More Details
CVE-2026-36611	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 returns 128 bytes of uninitialized buffer when receiving POST requests without SOAPAction header on UPnP port 1900, exposing internal memory to unauthenticated adjacent network attackers.	7.3	More Details
CVE-2026-11472	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. This affects an unknown function of the file /index1.php. This manipulation of the argument Password causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-11474	A security flaw has been discovered in Kushan2k student-management-system up to f16a4ceaddd6729c4b306ed4641cda3176c1ef2a. Affected is an unknown function of the file service/RegisterService.php of the component Registration Endpoint. Performing a manipulation of the argument stimg results in unrestricted upload. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-8876	Version 3.0.7 of the Securly Chrome Extension contains hardcoded, plaintext AES passphrases in securly.min.js. These keys decrypt crisis alert keyword data and intervention site data.	7.3	More Details
CVE-2026-10694	A vulnerability was detected in SourceCodester Online Food Ordering System 2.0. Affected by this issue is the function include of the file /index.php. The manipulation of the argument page results in file inclusion. The attack can be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-44186	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in the mod_proxy_ftp module in Apache HTTP Server with an attacker controlled backend FTP server. This issue affects undefined: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	7.3	More Details
CVE-2026-44185	Buffer Over-read vulnerability in Apache HTTP Server via outbound OCSP requests to an attacker controlled OCSP server This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	7.3	More Details
CVE-2026-10877	A security vulnerability has been detected in SourceCodester Ship Ferry Ticket Reservation System up to 1.0. This impacts an unknown function of the file /admin/login.php of the component Admin Login. Such manipulation of the argument Username leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-41567	Moby is an open source container framework. In versions prior to 29.5.1 and in moby/moby v2 prior to v2.0.0-beta.14, when a compressed archive is uploaded to a container via `PUT /containers/{id}/archive` or piped through `docker cp -`, the daemon resolves decompression binaries (such as `xz` or `unpigz`) from the container's filesystem rather than the host's due to incorrect ordering of operations. A malicious container image containing a trojanized decompression binary can achieve arbitrary code execution with full daemon privileges, including host root UID and unrestricted capabilities, when a user uploads a compressed (xz or gzip) archive into that container. This issue is fixed in Docker Engine 29.5.1 and moby/moby v2.0.0-beta.14. Workarounds include only running containers from trusted images, using authorization plugins to restrict access to the `PUT /containers/{id}/archive` endpoint, and avoiding piping compressed archives into containers created from untrusted images	7.2	More Details
CVE-2026-3820	There is a vulnerability in the Supermicro BMC SMTP service at Supermicro AS-2115HS-TNR. An attacker may obtain administrator privileges and inject specially crafted characters into the SMTP service configuration. This may cause the underlying system to execute unintended commands during process invocation. Potential impact includes denial-of-service attacks, arbitrary code execution, or permanent compromise of the controller.	7.2	More Details
CVE-2026-	The All-In-One Security (AIOS) – Security and Firewall plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 5.4.7. This is due to insufficient input sanitization in the get_rest_route() function and missing output escaping in the column_default() method of the debug log list table. When the 'Disable REST API for non-logged in users' feature (aiowps_disallow_unauthorized_rest_requests) is enabled alongside debug logging (aiowps_enable_debug), an unauthenticated attacker can embed arbitrary HTML or JavaScript in the REST request path. The path is retrieved via urldecode($_SERVER['REQUEST_URI']), which decodes URL-encoded payloads into literal HTML characters. This decoded, unsanitized value is concatenated directly	7.2	More

8438	into a debug log message and stored in the database. When an administrator navigates to the AIOS Dashboard Debug Logs page, the column_default() method returns the raw database value without escaping, and the parent list table echoes it directly, causing JavaScript execution in the administrator's browser session. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the debug log page, enabling nonce theft, privileged AJAX/REST actions, and potential full site compromise.		Details
CVE-2026-10727	An OS command injection vulnerability in Ivanti EPMM before 12.9.0.1, 12.8.0.3 and 12.7.0.2 versions allows a remote authenticated attacker to execute arbitrary commands as root	7.2	More Details
CVE-2026-8901	The Integration for Freshsales – Contact Form 7, WPForms, Elementor, Gravity Forms and More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Form Submission Data in all versions up to, and including, 1.0.15 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. The injected payload only executes when a CRM API call fails for the submitted form and an administrator subsequently views the error log details modal in the WordPress admin panel.	7.2	More Details
CVE-2026-7537	The MDJM Event Management plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.7.8.3 via the mdjm_send_comm_email function. This is due to no file type, extension, or MIME type validation being performed on uploaded files. This makes it possible for authenticated attackers, with administrator-level access and above, to upload files that may be executable, which makes remote code execution possible.	7.2	More Details
CVE-2026-50232	Lyrion Music Server 9.2.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts through media file metadata tags like GENRE, ARTIST, and ALBUM. Attackers can craft files with XSS payloads in metadata tags that execute in the web interface when users view track information or play files, enabling access to management functions and settings disclosure.	7.2	More Details
CVE-2026-50231	Lyrion Music Server 9.2.0 contains an unauthenticated stored cross-site scripting vulnerability in the log viewer that allows attackers to inject malicious scripts by exploiting unescaped template variables. Attackers can inject XSS payloads through search, lines, and path query parameters or by crafting values that get logged such as URLs, User-Agent headers, stream titles, or player names to execute arbitrary scripts in users' browsers.	7.2	More Details
CVE-2026-10586	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.1.3 via the `save_ai_generated_image()` 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.	7.2	More Details
CVE-2026-9851	The Booking Package plugin for WordPress is vulnerable to Privilege Escalation via Account Takeover in versions up to, and including, 1.7.16. This is due to a missing capability check on the 'updateUser' branch of the package_app_action AJAX endpoint, where the handler only validates a nonce and the dispatcher invokes Schedule::updateUser() with the $administrator argument hard-coded to 1, bypassing the only owner-restriction check inside that function and allowing the target user to be determined solely by attacker-supplied input passed directly to wp_update_user(). This makes it possible for authenticated attackers, with Editor-level access and above, to change the email address and password of any account, including Administrator accounts, resulting in a full site takeover.	7.2	More Details
CVE-2026-10843	A flaw was found in the OpenShift Cloud Credential Operator Mint-mode IAM policies for AWS. Operator credentials are provisioned with account-wide scope for destructive actions rather than being restricted to cluster-owned resources, enabling cross-scope impact after credential compromise.	7.2	More Details
CVE-2023-54351	WordPress Sonaar Music Plugin 4.7 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts through the comment functionality. Attackers can submit JavaScript payloads in the comment parameter to wp-comments-post.php which are stored and executed in the browsers of users viewing the affected playlist pages.	7.2	More Details
CVE-2026-11577	A flaw was found in Keycloak. A limited administrator can exploit an improper access control vulnerability in the POST /admin/realms/{realm}/partialImport endpoint. This allows them to bypass Fine-Grained Admin Permissions (FGAP) and escalate their privileges to a full realm administrator by importing users with realm-admin role mappings.	7.2	More Details
CVE-2019-25737	Live Chat Unlimited 2.8.3 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts through the chat input field. Attackers can submit payloads containing script tags and event handlers that execute in the admin area, enabling cookie theft or forced redirects to malicious websites.	7.2	More Details

CVE-2019-25731	Zuz Music 2.1 contains a persistent cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious JavaScript by submitting crafted contact form data. Attackers can inject script code through the name, subject, and message parameters in POST requests to /gmusic/zuzconsole/___contact, which executes when administrators view messages in the inbox interface.	7.2	More Details
CVE-2026-10870	A flaw has been found in Shibby Tomato 1.28.0000. This affects the function start_dhcpc of the file /sbin/rc of the component Web UI. This manipulation causes os command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. This project is superseded by FreshTomato.	7.2	More Details
CVE-2026-46492	md-fileserver allows for local viewing of markdown files in a browser. Prior to version 1.10.3, a cross-site scripting (XSS) vulnerability exists in the application's Markdown rendering logic. When user-supplied Markdown content is rendered, embedded raw HTML—including <script> tags—is processed and injected into the resulting page without sanitization, allowing arbitrary JavaScript execution in the context of the affected domain. This issue has been patched in version 1.10.3.	7.2	More Details
CVE-2026-10871	A vulnerability has been found in Shibby Tomato 1.28.0000. This vulnerability affects the function start_6rd_tunnel of the file /sbin/rc of the component Web UI. Such manipulation of the argument ipv6_6rd_borderrelay leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This project is superseded by FreshTomato.	7.2	More Details
CVE-2026-10873	A vulnerability was determined in Shibby Tomato 1.28.0000. Impacted is the function rstats_path of the file /bin/rstats of the component Web UI. Executing a manipulation can lead to os command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This project is superseded by FreshTomato.	7.2	More Details
CVE-2026-10872	A vulnerability was found in Shibby Tomato 1.28.0000. This issue affects the function start_vpnserver of the file /sbin/rc of the component Web UI. Performing a manipulation results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used. This project is superseded by FreshTomato.	7.2	More Details
CVE-2026-7556	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the comment text in all versions up to, and including, 7.5.49.7212 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. Exploitation requires an administrator to have enabled the non-default 'Parse Vimeo and YouTube links' (parse_comments) plugin setting, and requires a submitted comment to be approved by an administrator before the payload is publicly delivered.	7.2	More Details
CVE-2026-34194	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause mismanagement of a mapping state maintained for a sparse memory allocation. The product accidentally refers to the wrong memory due to the semantics of how math operations are implicitly scaled across buffers of different sizes.	7.1	More Details
CVE-2026-36606	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 encrypts configuration backups with a hardcoded DES key using single DES in ECB mode. An attacker who obtains a backup file can decrypt it to recover all stored credentials including admin password, WiFi PSK, and DDNS credentials.	7.1	More Details
CVE-2026-36176	GNCC GP5 v7.1.76 was discovered to store pre-signed Backblaze B2 upload URLs (PUT requests) in plaintext to the serial console. This allows physically-proximate attackers to extract these active tokens to perform unauthorized operations via monitoring the serial UART interface.	7.1	More Details
CVE-2026-45649	Improper access control in Office for Android allows an unauthorized attacker to perform spoofing locally.	7.1	More Details
CVE-2026-46657	Bludit is a content management system. Versions prior to 3.22.0 have a vulnerability in the user management logic that allows deactivated accounts to maintain access via persistent authentication tokens. When an administrator disables a user account, the application fails to invalidate or clear the associated tokenAuth and tokenRemember fields in the JSON database. Consequently, any user with a pre-existing "Remember Me" cookie can bypass the account disablement and maintain a valid authenticated state. Version 3.22.0 patches the issue.	7.1	More Details
CVE-2026-24349	A vulnerability has been identified in SIMATIC WinCC Unified PC Runtime V16 (All versions), SIMATIC WinCC Unified PC Runtime V17 (All versions), SIMATIC WinCC Unified PC Runtime V18 (All versions), SIMATIC WinCC Unified PC Runtime V19 (All versions), SIMATIC WinCC Unified PC Runtime V20 (All versions), SIMATIC WinCC Unified PC Runtime V21 (All versions < V21 Update 2). Insufficient protection of key material in WinCC Certificate Manager that could allow an attacker to extract sensitive information.	7.1	More Details

CVE-2026-11422	Markdown Preview Enhanced 0.8.x with crossnote engine 0.9.28 contains a code injection vulnerability in the WaveDrom rendering pipeline that allows attackers to execute arbitrary JavaScript by embedding malicious content in a wavedrom fenced code block within a crafted Markdown document. Attackers can exploit the unsanitized passing of wavedrom block content to window.eval() in the VS Code webview context to abuse the extension's message passing and invoke arbitrary file writes on the local filesystem.	7.1	More Details
CVE-2025-67448	The SMS module in Neterbit NW-431F Router 20241014-IR03 and before is vulnerable to stored XSS. The application does not properly sanitize user input in SMS messages before storing and displaying them. An attacker can send an SMS containing a malicious XSS payload, which will be executed in the context of the victim's browser when the message is viewed.	7.1	More Details
CVE-2026-49141	WACRM prior to commit 73041bf contain an authorization bypass vulnerability in the automation engine that allows authenticated attackers to access and modify contacts belonging to other tenants by supplying an arbitrary caller-controlled contact_id in the POST request body without tenant ownership verification. Attackers can exploit the service-role client that bypasses row-level security to modify victim contact fields including name, email, and company across tenant boundaries using only a known contact UUID.	7.1	More Details
CVE-2026-10840	A flaw was found in the OpenShift Pipelines operator. The tekton-scheduler-rolebinding ClusterRoleBinding grants the system:authenticated group write access to Kueue and cert-manager custom resources via the tekton-scheduler-role ClusterRole. When Kueue or cert-manager CRDs are present on the cluster, any authenticated user can disrupt workload scheduling, tamper with scheduling priorities, delete other tenants' Workload objects, or induce cert-manager to overwrite TLS Secrets including the default ingress controller certificate.	7.1	More Details
CVE-2026-44751	Application server ABAP does not perform necessary authorization checks for an authenticated user allowing an attacker to execute a report generation command which could overwrite information belonging to another user, resulting in escalation of privileges. This has high impact on integrity with low impact on availability and no impact on confidentiality of the application.	7.1	More Details
CVE-2025-15654	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fox-themes Prague allows Reflected XSS. This issue affects Prague: from n/a through 2.2.8.	7.1	More Details
CVE-2016-20063	Single Personal Message 1.0.3 contains an SQL injection vulnerability that allows authenticated users to execute arbitrary SQL queries by injecting malicious code through the message parameter. Attackers can access the admin interface and supply crafted SQL statements in the message parameter to extract sensitive database information including user credentials and site configuration data.	7.1	More Details
CVE-2026-48569	Improper input validation in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	7.1	More Details
CVE-2026-41845	Due to incorrect escaping, the use of JavaScriptUtils.javaScriptEscape() may lead to JavaScript code injection in the browser, potentially resulting in a cross-site scripting (XSS) vulnerability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	7.1	More Details
CVE-2026-11269	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker in a privileged network position to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	7.1	More Details
CVE-2026-8874	Version 3.0.7 of the Securly Chrome Extension downloads JSON files containing crisis alert keywords and filtering rules over unencrypted HTTP via the Fetch API. Other endpoints in the same extension correctly fetch IWF and CIPA data over HTTPS, demonstrating an inconsistent implementation of TLS.	7.1	More Details
CVE-2026-48507	Snipe-IT is an IT asset/license management system. A vulnerability in versions prior to 8.6.0 allows a non-admin user holding only the granular `users.edit` permission to lock every admin out of the instance by editing the `activated` flag (which determines whether or not a user can login) and the `ldap_import` flag, which determines whether or not the user can request a password reset. Version 8.6.0 contains a patch.	7.1	More Details
CVE-2025-52612	HCL iControl was affected by Export CSV - CSV Injection vulnerability. It is vulnerable to a reflected cross-site scripting vulnerability. This was caused by an insufficient sanitation of input parameters. .	7.1	More Details
CVE-2026-47288	Integer overflow or wraparound in Windows Kerberos allows an authorized attacker to execute code over an adjacent network.	7.1	More Details

CVE-2026-47648	Untrusted search path in Windows Storage allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-47293	Use after free in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-42911	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-42912	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45603	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-42984	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-44818	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.0	More Details
CVE-2026-42836	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45596	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45597	Concurrent execution using shared resource with improper synchronization ('race condition') in UI Automation Manager (uiamanager.dll) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45598	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45601	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-41108	Heap-based buffer overflow in Microsoft Windows DNS allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45640	Use after free in Windows Bluetooth Port Driver allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-34335	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45653	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-45608	Out-of-bounds read in Windows DHCP Server allows an authorized attacker to disclose information locally.	6.8	More Details
CVE-2026-36175	An issue in the U-Boot component of GNCC GP5 v7.1.76 allows physically-proximate attackers to bypass authentication and gain root access via interrupting the boot sequence and injecting a crafted string into the kernel boot arguments.	6.8	More Details

CVE-2026-50206	Incoming VPN network profile settings fail to process special characters safely, enabling command injection via malicious config files.	6.8	More Details
CVE-2026-11628	Use after free in Ozone in Google Chrome prior to 149.0.7827.103 allowed a local attacker to potentially exploit heap corruption via physical access to the device. (Chromium security severity: Critical)	6.8	More Details
CVE-2026-7764	An out-of-bounds read vulnerability in the morse.ko HaLow Wi-Fi kernel driver in Morse Micro HaLowLink 2 software versions prior to 2.11.12 allows an unauthenticated attacker within radio range to disclose a small amount of kernel heap memory or cause a Denial of Service (kernel oops/panic) via a crafted 802.11ah beacon or probe response frame containing a malformed Vendor Information Element. The function morse_vendor_find_vendor_ie() does not validate the IE length against the expected structure size before its result is passed to morse_vendor_rx_caps_ops_ie() and morse_vendor_fill_sta_vendor_info(), which read at fixed offsets into the IE data. Because the length check only requires the IE to be longer than 3 bytes, an attacker can supply an undersized IE, causing a heap out-of-bounds read of up to 9 bytes. No authentication, association, or user interaction is required.	6.8	More Details
CVE-2026-11166	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.8	More Details
CVE-2026-50507	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	6.8	More Details
CVE-2026-11218	Inappropriate implementation in PlatformIntegration in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a malicious file. (Chromium security severity: Low)	6.8	More Details
CVE-2025-67862	An Internal Asset Exposed to Unsafe Debug Access Level or State vulnerability [CWE-1244] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.2, FortiOS 7.4.0 through 7.4.7, FortiOS 7.2.0 through 7.2.10, FortiOS 7.0.0 through 7.0.16, FortiOS 6.4 all versions, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0 all versions may allow an authenticated admin to execute lua scripts via crafted CLI commands.	6.7	More Details
CVE-2026-10805	A flaw was found in NetworkManager. This local privilege escalation vulnerability exists in NetworkManager's dhclient backend when processing malformed Manufacturer Usage Description (MUD) URLs. A local user can exploit this flaw to escalate privileges by triggering a script via a crafted MUD URL, provided an administrator has explicitly configured NetworkManager to use dhclient. This issue does not affect default configurations of NetworkManager.	6.7	More Details
CVE-2026-44754	The Remote Function Call (RFC) modules of the Operational Data Provisioning Data Replication API (ODP-RFC) are missing caller identification of permitted SAP-internal applications and are being used by customer or third-party applications in ways that are not aligned with its intended usage. Which could lead to unintended disclosure of data, but does not affect integrity, and poses minimal availability concerns for the application.	6.6	More Details
CVE-2026-7566	The LearnPress – Backup & Migration Tool plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.1.4 via deserialization of untrusted input . This makes it possible for authenticated attackers, with administrator-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.	6.6	More Details
CVE-2026-41976	Permission control vulnerability in the audio framework. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.6	More Details
CVE-2026-11658	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-11653	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-	7-Zip is a file archiver with a high compression ratio. Versions 9.21 through 26.00 contain an An uninitialized memory disclosure vulnerability in the UEFI capsule (.scap) parser in 7-Zip. The OpenCapsule		

2026-48101	function allocates a heap buffer of attacker-declared CapsuleImageSize (up to 1 GiB) without zero-initialization, then reads the file contents into it with ReadStream_FALSE whose return value is silently discarded. If the file is truncated, the unread tail of the buffer retains uninitialized heap memory, which is then exposed as extracted file content via GetStream. Version 26.0.1 fixes the issue.	6.5	More Details
CVE-2026-9829	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to time-based SQL Injection via 'compact_album_order_by' Shortcode Parameter in all versions up to, and including, 1.8.41 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The malicious payload is stored via the 'shortcode_bwg' AJAX handler — accessible to Contributor-level users and exploitable without a valid nonce by omitting the 'page' parameter — and is subsequently triggered by the unauthenticated 'bwg_frontend_data' AJAX handler, meaning successful exploitation requires only that an attacker has Contributor-level access to save the shortcode.	6.5	More Details
CVE-2026-43951	Out-of-bounds Read vulnerability in Apache HTTP Server with mod_headers and mod_mime and multiple response languages. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67.	6.5	More Details
CVE-2025-5089	In a CVX cluster, an EOS switch connected to a CVX server is not resilient to certain malformed messages received from the connected CVX server. Similarly, the CVX server is not resilient to certain malformed messages received from the connected EOS switch. This leads to either a Sysdb agent crash on the EOS device causing a soft reset of the switch or agent crashes on the CVX server causing instability of the CVX cluster. An attacker could use this behavior to create a denial of service (DoS) scenario. Note that this would require the attacker to already have a high privilege access to the connected device to be able to send custom TCP packets. EOS switches that are not connected to a CVX server are not impacted.	6.5	More Details
CVE-2026-10786	Improper access control in the ticketing integration settings in Devolutions Server allows an authenticated low-privileged user to obtain cleartext credentials for configured ticketing integrations via a crafted API request. This issue affects : * Devolutions Server 2026.2.4.0 * Devolutions Server 2026.1.20.0 and earlier	6.5	More Details
CVE-2025-5090	CVX is not resilient to unexpected messages from a connected switch. This leads to agent crashes on CVX causing instability in the CVX cluster. An attacker could use this behavior to create a denial of service (DoS) scenario. Note that this would require the attacker to have a high privilege access to the connected switch to be able to send custom TCP packets to the CVX.	6.5	More Details
CVE-2026-46397	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, an Authenticated Local File Inclusion (LFI) vulnerability in the HAXCMS saveOutline endpoint allows a low-privileged user to read arbitrary files on the server by manipulating the location field written into site.json. This enables attackers to exfiltrate sensitive system files such as /etc/passwd, application secrets, or configuration files accessible to the web server (www-data). Version 26.0.0 patches the issue.	6.5	More Details
CVE-2026-48112	7-Zip is a file archiver with a high compression ratio. Versions 9.18 through 26.00 contain a heap out-of-bounds read in 7-Zip Ar handler BSD SYMDEF parser. A 4-byte heap out-of-bounds read exists in the Unix ar archive parser in 7-Zip. When parsing a BSD-style __.SYMDEF symbol table, the ParseLibSymbols function reads a 32-bit namesSize field via Get32 at a position that can equal the buffer size, reading 4 bytes past the end of the heap allocation. This reads uninitialized heap data under the default allocator. Version 26.01 patches the issue.	6.5	More Details
CVE-2026-46357	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, the HAX CMS NodeJS application crashes when an authenticated attacker sends a specially crafted site creation request to the createSite endpoint. A single request is sufficient to take the entire application offline, requiring a manual server restart to restore service. Version 26.0.0 fixes the issue.	6.5	More Details
CVE-2026-44744	SAP S/4HANA(On-Premise) contains SQL injection vulnerability in a remote-enabled function module component that could be exploited by an authenticated attacker to potentially execute unauthorized database queries.This flaw exposes sensitive information to which they should not otherwise have access to. The vulnerability has a high impact on the confidentiality of the data with no impact on the integrity and availability of the application.	6.5	More Details
CVE-2020-37248	OfflineIMAP before 8.0.3 trusts the server with their STARTTLS capability prior to authentication, which allows STRIPTLS/man-in-the-middle attacks, taking over the connection and extracting account credentials in cleartext.	6.5	More Details
CVE-2026-10544	Improper neutralization of special elements in the built-in PAM provider password rotation templates in Devolutions Server allows an authenticated user with write access to a vault to execute arbitrary commands on the systems managed by the affected PAM provider. This issue affects : * Devolutions Server 2026.2.4.0 * Devolutions Server 2026.1.20.0 and earlier	6.5	More Details

CVE-2026-39908	OpenBullet2 through version 0.3.2 on Windows contains a credential disclosure vulnerability that allows remote attackers to capture the NTLMv2 hash of the process user by configuring a job proxy source with a UNC path pointing to an attacker-controlled server. When the job starts, the application attempts to load proxies from the UNC path, triggering an SMB authentication attempt that discloses the NTLMv2 hash, which can then be relayed or cracked offline.	6.5	More Details
CVE-2026-11611	A flaw was found in 389 Directory Server. The Content Synchronization persistent search plugin allows unbounded memory growth when an authenticated client stops reading sync responses, enabling denial of service. Additional race conditions in plugin thread lifecycle can cause crashes during connection teardown or shutdown.	6.5	More Details
CVE-2026-9754	An authenticated user with the read role may read limited amounts of uninitialized stack memory via specially-crafted issuances of the filemd5 command	6.5	More Details
CVE-2026-11089	Uninitialized Use in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11087	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11051	Out of bounds read in ANGLE in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11081	Inappropriate implementation in Canvas in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11078	Inappropriate implementation in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11075	Out of bounds read in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11073	Use after free in WebGL in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11069	Insufficient validation of untrusted input in Cast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11067	Uninitialized Use in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11064	Race in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11057	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11048	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11084	Inappropriate implementation in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11045	Insufficient validation of untrusted input in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE-2026-11044	Integer overflow in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11039	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11038	Insufficient policy enforcement in Subresource Integrity in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via malicious network traffic. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11036	Inappropriate implementation in DOM in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11033	Uninitialized Use in WebML in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11032	Inappropriate implementation in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11027	Insufficient validation of untrusted input in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11083	Inappropriate implementation in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-37737	sanic-cors version 2.2.0 and prior contains an improper regular expression in the try_match() function in sanic_cors/core.py that uses re.match without end-anchoring. This allows an attacker to bypass CORS origin allowlists by registering a domain that begins with a trusted origin string, to gain unauthorized access to cross-origin requests for authenticated resources.	6.5	More Details
CVE-2026-11025	Insufficient policy enforcement in Navigation in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11109	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11132	Insufficient policy enforcement in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11129	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-26824	libxls through version 1.6.3 contains a use of uninitialized memory vulnerability in the OLE container parser. Memory allocated for the Master Sector Allocation Table (MSAT) in read_MSAT() is not fully initialized before being consumed by ole2_validate_sector_chain(), which may result in application crashes or potential information disclosure when processing a crafted XLS file	6.5	More Details
CVE-2026-11128	Inappropriate implementation in Web Share in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11127	Inappropriate implementation in WebAPKs in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted WebAPK. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11123	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-	Insufficient validation of untrusted input in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML	6.5	More

11121	page. (Chromium security severity: Medium)		Details
CVE-2026-11110	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-8722	Net::Async::Statsd::Client versions through 0.005 for Perl allow metric injections. The metric names are not checked for newlines, colons or pipes. Metrics generated from untrusted sources could inject additional statsd metrics.	6.5	More Details
CVE-2026-11090	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-8653	The MasterStudy LMS Pro Plus plugin for WordPress is vulnerable to generic SQL Injection via the 'columns' parameter in all versions up to, and including, 4.8.20 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 instructor-level access or 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-2026-11106	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11105	Insufficient validation of untrusted input in WebUI in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11104	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11101	Uninitialized Use in Dawn in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11097	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11096	Out of bounds read in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11093	Inappropriate implementation in Printing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11026	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11023	Inappropriate implementation in WebAppInstalls in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11135	Insufficient policy enforcement in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-10937	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2019-25740	Joomla com_jsjobs 1.2.6 contains an arbitrary file deletion vulnerability that allows authenticated attackers to delete files by manipulating custom userfield parameters. Attackers can send POST requests to the job.savejob task with path traversal sequences in the field_2 parameter to delete arbitrary files accessible to the web server.	6.5	More Details
CVE-2026-	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted video	6.5	More Details

10981	file. (Chromium security severity: High)		
CVE-2026-10980	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-10979	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-10977	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-10950	Insufficient policy enforcement in Autofill in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-10944	Insufficient policy enforcement in Autofill in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-10938	Inappropriate implementation in Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-45501	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-10992	Insufficient data validation in Animation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-10912	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-42539	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 return sensitive data to the user which are not required for the client’s operation. Version 2.4.28 contains a patch.	6.5	More Details
CVE-2026-11322	Hermes WebUI prior to v0.51.221 contains a path traversal vulnerability that allows attackers to escape the workspace boundary by supplying symlinks that resolve to files or directories outside the designated workspace root. Attackers can exploit the workspace file and listing APIs, which resolve symlink targets without enforcing that the final path remains within the workspace, to read external host files accessible to the server process and disclose sensitive data such as SSH keys, cloud credentials, or application tokens.	6.5	More Details
CVE-2024-6858	In Arista’s EOS when in 802.1X mode, multi-auth unauthenticated hosts might be allowed access to a switch port if there exists an EAPOL capable device in the fallback VLAN.	6.5	More Details
CVE-2026-36499	A missing upper-bound check in the udpif_set_threads() function of Open vSwitch v3.6.90 allows an attacker with OVSDB write access to request an excessive number of handler or revalidation threads. This can cause a denial of service (DoS) via resource exhaustion.	6.5	More Details
CVE-2026-49940	Net::CIDR::Set versions through 0.20 for Perl accept non-ASCII IP addresses and netmasks. Unicode digits such as the Arabic-Indic One (U+0661) were accepted but not properly parsed as numbers. This could allow network masks to accept larger networks.	6.5	More Details
CVE-2026-47284	Exposure of sensitive information to an unauthorized actor in Visual Studio Code allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-10860	A logic error in the MISP CRUD component delete handler allowed validation failures to be bypassed when requests used the HTTP DELETE method. Due to missing parentheses in the delete condition, the expression was evaluated as ($validationError === null && POST) || DELETE, meaning a DELETE request could proceed even when the delete validation callback had rejected the operation. An authenticated attacker with access to an affected delete endpoint could abuse this flaw to delete records that should have been protected by application-level validation or authorization checks.	6.5	More Details

CVE-2026-10985	Out of bounds read in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-10993	Heap buffer overflow in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11022	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11008	Insufficient validation of untrusted input in WebAppInstalls in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11020	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted XML file. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11019	Inappropriate implementation in Payments in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11018	Insufficient policy enforcement in Actor in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11017	Inappropriate implementation in Link Preview in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11016	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-49204	Leftover debug modules contain fixed credentials for internal AWS Cognito test sandboxes, risking asset exploitation.	6.5	More Details
CVE-2026-11014	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11013	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11007	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-10994	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11006	Out of bounds read in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11001	Inappropriate implementation in Payments in Google Chrome prior to 149.0.7827.53 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-2026-10999	Integer overflow in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-	Weak validation logic within device dissociation API routines allows a remote entity to forcefully unbind unrelated user endpoints, causing severe denial of service.	6.5	More Details

50212			
CVE-2026-50508	Exposure of sensitive information to an unauthorized actor in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-10997	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-10996	Inappropriate implementation in Workers in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-49956	Hermes WebUI before version 0.51.269 contains a profile isolation bypass vulnerability that allows authenticated users to access data belonging to other profiles by querying the session search endpoint without active-profile filtering. Attackers can send requests to the sessions search handler to retrieve session titles and transcript message content from profiles other than their own active profile.	6.5	More Details
CVE-2026-11134	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11133	Insufficient policy enforcement in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11137	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11275	Inappropriate implementation in Page Info in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11299	Integer overflow in Fonts in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11289	Side-channel information leakage in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11288	Insufficient policy enforcement in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11287	Insufficient policy enforcement in Navigation in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11284	Side-channel information leakage in PerformanceAPIs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11283	Insufficient validation of untrusted input in Shortcuts in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11278	Inappropriate implementation in CustomTabs in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-42903	Null pointer dereference in Windows Kerberos allows an authorized attacker to deny service over a network.	6.5	More Details
CVE-2026-42907	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information locally.	6.5	More Details
CVE-	Insufficient policy enforcement in PreviewTab in Google Chrome on Android prior to 149.0.7827.53		

2026-11226	allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11271	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11270	Inappropriate implementation in UI in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11268	Uninitialized Use in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11263	Insufficient policy enforcement in WebAuthentication in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11258	Inappropriate implementation in File System Access in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-47655	Exposure of sensitive information to an unauthorized actor in Microsoft Graph allows an authorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-36604	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 does not validate the HTTP Host header, enabling DNS rebinding attacks. An external attacker can rebind a domain to the router's internal IP address, extending the CORS wildcard vulnerability (Access-Control-Allow-Origin: *) to internet-originated attacks.	6.5	More Details
CVE-2026-47644	Improper neutralization of special elements in output used by a downstream component ('injection') in Copilot Chat (Microsoft Edge) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2019-25720	Dräger SC Monitoring devices (SC 6002XL, SC 6802XL, SC 7000, SC 8000, SC 9000 XL) contain a denial-of-service vulnerability in all software versions that allows unauthenticated attackers to reboot the monitor by sending a malformed network packet. Attackers can repeatedly send such malformed packets to disrupt patient monitoring until the device falls back to default configuration and loses network connectivity.	6.5	More Details
CVE-2025-70101	An out-of-bounds read in the ext4_ext_binsearch_idx function in src/ext4_extent.c of the lwext4 1.0.0 library allows attackers to cause a denial of service by supplying a specially crafted ext4 filesystem image. The vulnerability occurs due to insufficient validation of extent header fields before performing a binary search over extent index entries, which can result in invalid pointer calculations and an out-of-bounds memory read during extent tree traversal.	6.5	More Details
CVE-2026-49938	A improper access control vulnerability in Fortinet FortiPortal 7.4.0 through 7.4.7, FortiPortal 7.2.0 through 7.2.8, FortiPortal 7.0 all versions may allow attacker to improper access control via <insert attack vector here>	6.5	More Details
CVE-2026-25657	Ericsson Packet Core Gateway (PCG) versions prior to 1.30 contain an Improper Handling of Syntactically Invalid Structure (CWE-228) vulnerability where an attacker continuously sending a specially crafted message can cause service degradation. The impact continues as long the attack persists but the system recovers from the crashes when the attack stops.	6.5	More Details
CVE-2026-33582	Unrestricted Upload of File with Dangerous Type vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. A crafted TIFF image could trigger excessive memory allocation during image decoding, allowing an authenticated user to cause the server process to crash. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	6.5	More Details
CVE-2026-34031	Unrestricted Upload of File with Dangerous Type vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. The server did not sufficiently validate user-supplied image URLs, allowing arbitrary external content to be embedded as profile images, which could expose users to unintended external requests and tracking by third-party servers. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	6.5	More Details
CVE-2025-59174	Ericsson Packet Core Controller (PCC) versions prior to 1.39 contain a vulnerability where an attacker sending a large volume of specially crafted messages may cause service degradation.	6.5	More Details

CVE-2026-34905	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. The unlisted question feature did not enforce access restrictions on direct API endpoints, allowing authenticated users to discover and access unlisted questions, their answers, comments, and revision history. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	6.5	More Details
CVE-2026-49818	The Apache Airflow Samba provider's `GCSToSambaOperator` joined GCS object names to the SMB destination path without a containment check, so an object named with `../` segments resolved a write path outside the configured `destination_path`. An attacker able to write objects into the source GCS bucket — typically an external data producer distinct from the trusted DAG author — could write files to arbitrary locations on the Samba target when the operator ran. Upgrade apache-airflow-providers-samba to 4.12.6 or later, which validates the resolved destination stays within `destination_path`.	6.5	More Details
CVE-2026-7542	The Slider Revolution plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to and including 7.0.10. This is due to three compounding design flaws: (1) the plugin leaks a valid backend AJAX nonce (revslider_actions) to all authenticated users including Subscribers via the admin_footer hook; (2) the wordpress.create.image_from_url action is explicitly allowlisted in the $user_allowed array, bypassing the administrator-only access control; (3) the create_wordpress_image_from_url() function accepts an attacker-controlled url parameter that is passed to import_media(), where path_or_url_exists() explicitly accepts local filesystem paths (file_exists() && is_readable()) with no restriction to remote HTTP/HTTPS URLs, and @copy() physically copies those files into the publicly accessible /wp-content/uploads/revslider/ai/ directory. The MIME type check trusts the attacker-supplied content_type parameter to derive the destination extension without verifying actual file content, and the source extension blacklist does not block many sensitive types (.sql, .log, .json, .bak, .xml, .csv, .conf, .yml, .yaml, .pem, .key, .crt, .txt, .db, etc.). This makes it possible for authenticated attackers with Subscriber-level access and above to read the contents of server files with non-blacklisted extensions by having them copied to a publicly accessible URL.	6.5	More Details
CVE-2026-9752	An authorized user could trigger a server crash by running a query with a 2dsphere index on a field that stores a GeoJSON GeometryCollection containing a Polygon with a strict-winding CRS. Strict-winding polygons are intentionally unsupported for indexing, but the guard that rejects them does not inspect members of a GeometryCollection, allowing the unsafe path to be reached which ends with an ensuing null-pointer dereference.	6.5	More Details
CVE-2026-9750	An authenticated user can cause a MongoDB server to crash or return incorrect results by creating documents that interfere with internal metadata processing during query execution. This stems from insufficient separation between user-controlled document fields and internal metadata in certain execution paths.	6.5	More Details
CVE-2026-9749	This issue can occur when running an aggregation pipeline that uses the internal $exchange stage configured with key-range partitioning and order-preserving delivery. If a single key range produces enough documents to fill its exchange buffer (that is, many results are routed to the same consumer), the server reaches the code path where a full per-consumer buffer is detected but the internal "high watermark" for that key range is not updated as intended.	6.5	More Details
CVE-2026-9748	The $_internalConvertBucketIndexStats stage used PauseExecution as a way to signal "skip this document" when an index stats conversion failed. But PauseExecution is not a general purpose skip mechanism, but rather a TeeBuffer-internal signal used solely by $facet to coordinate its sub-pipelines. When this stage is placed before $facet in a pipeline, TeeBuffer receives the unexpected PauseExecution from upstream and hits a hard invariant assertion, crashing mongod.	6.5	More Details
CVE-2026-9747	Adding fromRouter:true and runtimeConstants.userRoles could cause aggregations to crash mongodb server.	6.5	More Details
CVE-2026-9746	When using $changestreams and $_requestReshardingResumeToken with the exchange option the server hits an invariant which causes the server to crash. There are no special privileges needed. The user must be logged in to issue the statement.	6.5	More Details
CVE-2026-9743	In MongoDB Server 8.0, an aggregation stage can leave its _subPipeline field null during processing of certain pipelines. If a getMore is subsequently issued on the same cursor, the server may dereference this null sub-pipeline when reattaching to the operation context, accessing an invalid address and crashing the process. This issue allows an authenticated user who can run aggregation pipelines to cause a denial of service by issuing a specially crafted aggregation followed by getMore on affected versions.	6.5	More Details
CVE-2026-9741	A bug in query analysis processing of the $vectorSearch aggregation stage for Queryable Encryption (QE) or Client-Side Field Level Encryption (CSFLE) results in literal values for encrypted fields within the $vectorSearch stage filter expressions to be sent to the server as plaintext instead of ciphertext.	6.5	More Details
	lldpd is an implementation of IEEE 802.1ab (LLDP). Prior to version 1.0.22, lldpd_decode() in		

CVE-2026-46433	src/daemon/lldpd.c strips 802.1Q VLAN tags from received Ethernet frames by calling memmove() to shift the frame payload 4 bytes left. The third argument (byte count) is s - 2 * ETHER_ADDR_LEN but should be s - 2 * ETHER_ADDR_LEN - 4, causing a 4-byte heap buffer over-read past the malloc(h_mtu) allocation when the received frame size equals the interface MTU. This issue has been patched in version 1.0.22.	6.5	More Details
CVE-2026-25659	Ericsson Packet Core Gateway (PCG) versions prior to 1.30 contain an Improper Handling of Missing Values (CWE-230) vulnerability where an attacker continuously sending a specially crafted message can cause service degradation. The impact continues as long the attack persists but the system recovers from the crashes when the attack stops.	6.5	More Details
CVE-2026-25658	Ericsson Packet Core Gateway (PCG) versions prior to 1.30 contain an Improper Handling of Missing Values (CWE-230) vulnerability where an attacker continuously sending a specially crafted message can cause service degradation. The impact continues as long the attack persists but the system recovers from the crashes when the attack stops.	6.5	More Details
CVE-2026-11227	Incorrect security UI in Tab Hover Cards in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Low)	6.5	More Details
CVE-2026-42824	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-36605	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 is vulnerable to a HTTP denial of service via a low number of crafted incomplete HTTP requests, causing a persistent crash that requires physical power cycling to recover.	6.5	More Details
CVE-2026-11195	Inappropriate implementation in MHTML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11193	Insufficient policy enforcement in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11190	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11189	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11183	Out of bounds read in GWP-ASan in Google Chrome prior to 149.0.7827.53 allowed a local attacker to obtain potentially sensitive information from process memory via a malicious file. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11182	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11180	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11176	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11168	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11160	Out of bounds read in Input in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-45454	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	6.5	More Details
CVE-			

2026-11148	Inappropriate implementation in Payments in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11143	Out of bounds read in Extensions in Google Chrome on Linux prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11142	Insufficient policy enforcement in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11141	Uninitialized Use in Audio in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11140	Out of bounds read in Chromecast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11139	Inappropriate implementation in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11138	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2025-55659	A NULL pointer dereference in the ctts_box_write function (isomedia/box_code_base.c) of GPAC MP4Box v2.4 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MP4 file.	6.5	More Details
CVE-2025-55658	GPAC MP4Box v2.4 was discovered to contain a floating point exception in the gf_opus_parse_packet_header function (media_tools/av_parsers.c). bThis vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	6.5	More Details
CVE-2026-11225	Inappropriate implementation in WebUI in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11194	Inappropriate implementation in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11210	Inappropriate implementation in Safe Browsing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted RAR file. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11209	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-26379	Koha versions up to 25.11 contain a Server-Side Request Forgery (SSRF) vulnerability via the Z39.50/SRU server configuration. This allows authenticated attackers to perform internal network scanning and identify running services by analyzing server response times.	6.5	More Details
CVE-2026-11223	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-36724	An uncaught exception in the /application/job/update/{id} endpoint of FastapiAdmin v2.2.0 allows authenticated attackers with the module_task:job:update permission to cause a Denial of Service (DoS) via manipulating the func field of scheduled tasks.	6.5	More Details
CVE-2026-11222	Incorrect security UI in Tab Strip in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11220	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details

CVE-2026-11217	Inappropriate implementation in Fenced Frames in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-11215	Inappropriate implementation in Cronet in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11214	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11196	Type Confusion in XML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted XML file. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-47287	Relative path traversal in Visual Studio Code allows an unauthorized attacker to perform tampering over a network.	6.5	More Details
CVE-2026-11208	Use after free in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11206	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11204	Inappropriate implementation in Signin in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11203	Inappropriate implementation in GPU in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11200	Inappropriate implementation in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-11197	Insufficient policy enforcement in Workers in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-3011	The Recipe Card Blocks Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the recipe block's 'summary' and 'notes' attributes in all versions up to, and including, 3.4.13. This is due to the 'WPZOOM_Helpers::deserialize_block_attributes' method converting unicode-encoded sequences back into HTML characters after sanitization has already been applied. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that execute whenever a user accesses the published post or the print view of an injected recipe.	6.4	More Details
CVE-2019-25743	WordPress Soliloquy Lite 2.5.6 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by inserting script tags in the post title field. Attackers can submit POST requests to the post editing endpoint with script payloads in the post_title parameter, which are stored and executed when users preview the post.	6.4	More Details
CVE-2019-25742	WordPress Theme Zoner Real Estate 4.1.1 contains a persistent cross-site scripting vulnerability that allows authenticated agents to inject malicious scripts through the Address input field when creating properties. Attackers can inject JavaScript payloads in the property creation form that execute when administrators view the property for approval, enabling cookie theft and session hijacking.	6.4	More Details
CVE-2026-36612	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 enables WPS 2.0 by default with a weak lockout policy (60-second lockout after 10 attempts).	6.4	More Details
CVE-2019-25744	WordPress Popup Builder 3.49 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by breaking out of option tags in the post_title parameter. Attackers can submit crafted POST requests to the post.php endpoint with script payloads in the post_title field that execute when pages or posts display popup selections.	6.4	More Details
	GigToDo 1.3 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to		

CVE-2019-25739	inject malicious JavaScript and HTML code through the proposal description field. Attackers can craft XSS payloads in the create_proposal endpoint that execute when administrators or other users view the stored proposal, enabling cookie theft and malicious redirects.	6.4	More Details
CVE-2026-41982	Race condition vulnerability in the IPC module. Impact: Successful exploitation of this vulnerability may affect availability.	6.4	More Details
CVE-2021-47984	WordPress Plugin WP24 Domain Check 1.6.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the fieldnameDomain parameter. Attackers can inject JavaScript payloads through the plugin settings form at options.php that execute in the browsers of administrators viewing the settings page.	6.4	More Details
CVE-2026-8599	The MailerPress – Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Campaign HTML Content Field in all versions up to, and including, 2.0.4 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. The public-facing campaign preview endpoint (/mp-email/{id}-slug/) is not affected by this vulnerability, as it applies a Content-Security-Policy header blocking all inline scripts; exploitation is limited to the admin dashboard preview.	6.4	More Details
CVE-2026-50592	In Znuny LTS before 6.5.21 and Znuny before 7.3.3, there is reflected XSS in AdminCommunicationLog (aka the communication log administration view).	6.4	More Details
CVE-2026-10738	The jQuery Hover Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Footnote Qualifier ('{{...}}' Syntax) in all versions up to, and including, 1.4 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. The attribute-breakout payload (e.g., a double-quote followed by an event handler) contains no angle brackets and therefore bypasses WordPress core's wp_kses_post() filtering, which only strips disallowed HTML tags rather than sanitizing attribute contexts.	6.4	More Details
CVE-2026-10024	The TinyMCE shortcode Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'btnrel' Shortcode Attribute in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5714	The Enable Media Replace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘location_dir’ parameter in all versions up to, and including, 4.1.8 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-2021-47983	WordPress Plugin Stripe Payments 2.0.39 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the AcceptStripePayments-settings[currency_code] parameter. Attackers can submit POST requests to /wp-admin/options.php with script payloads in the currency_code field to execute arbitrary JavaScript in administrator browsers when settings are viewed.	6.4	More Details
CVE-2026-7662	The ePaperFlip Publisher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'publicationid' attribute of the `epaperflip_embed` shortcode in all versions up to, and including, 1. This is due to insufficient input sanitization and output escaping on the shortcode attribute which is injected directly into inline JavaScript. 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-2026-10862	The Accordions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Accordion body field in all versions up to, and including, 2.3.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Custom-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-2026-8893	The Express Payment For Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' attribute of the [stripe-express] shortcode in versions up to, and including, 1.28.0. This is due to insufficient input sanitization and output escaping on the shortcode attribute value, which is concatenated into an HTML attribute in the rendered output of the register_shortcode() function without being passed through esc_attr() or any other escaping function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2026-8900	The Simple SEO Slideshow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.2.8 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. WordPress KSES does not strip malicious shortcode attribute values on post save, allowing contributor-level users to persist payloads that execute for any visitor, including administrators reviewing the post.	6.4	More Details
CVE-2026-8677	The Prime Elementor Addons – Lightweight Elementor Widgets for Faster Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Widget HTML Tag Settings in all versions up to, and including, 1.3.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit succeeds even for users without the unfiltered_html capability because the payload (e.g., 'img src=x onerror=alert(document.domain)') contains no HTML angle brackets and therefore passes through Elementor's wp_kses_post() filter unchanged at save time.	6.4	More Details
CVE-2026-9281	The Master Addons For Elementor – Widgets, Extensions, Theme Builder, Popup Builder & Template Kits plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'jtlma_custom_js' Page Setting (Custom JS Extension) in all versions up to, and including, 3.1.0 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. The unfiltered_html capability check is only enforced during Elementor control registration (UI rendering) and not during the save process, enabling Author-level users to inject the jtlma_custom_js setting directly via a crafted POST request to admin-ajax.php?action=elementor_ajax, bypassing the UI-level restriction entirely.	6.4	More Details
CVE-2026-8841	The Extra Settings for RocketChat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rocketchat' shortcode's 'title' attribute in versions up to, and including, 0.1. This is due to insufficient input sanitization and output escaping in the rxstg_shortcode() function, which concatenates the user-supplied 'title' attribute directly into HTML output. 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-2026-7795	The Click to Chat – WA Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the [chat] shortcode 'num' parameter in all versions up to, and including, 4.38. This is due to insufficient escaping when embedding user-supplied shortcode attribute values inside JavaScript string literals that are then placed in HTML event-handler attributes. The CCW_Shortcode::shortcode() function applies esc_attr() to the 'num' parameter (line 157), which converts single quotes to the HTML entity '. This entity-encoded value is then interpolated directly into a JavaScript window.open() call string delimited by single quotes (line 194/221), and that complete string is placed verbatim into an HTML onclick attribute in the style template files (e.g., sc-style-1.php line 6). Because browsers HTML-decode event attribute values before executing the embedded JavaScript, the ' entities are decoded back to literal single quotes at runtime, allowing the injected payload to break out of the JavaScript string context and execute arbitrary code. This makes it possible for authenticated attackers with Contributor-level access and above to inject arbitrary web scripts into pages that will execute whenever a user clicks the WhatsApp chat button rendered by the [chat] shortcode.	6.4	More Details
CVE-2026-7796	The EmbedPress – PDF Embedder, Embed PDF viewer, YouTube Videos, 3D FlipBook, Social feeds & more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the block 'url' attribute in all versions up to, and including, 4.5.3 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-2026-8880	The RomanCart Ecommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'blclass' attribute (and other attributes) of the romancart_button shortcode in versions up to, and including, 2.0.8. This is due to insufficient input sanitization and output escaping on user supplied attributes within the romancart_button_shortcode() function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-8882	The WP ApplicantStack Jobs Display plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-	The Global Body Mass Index Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gbmicalc' shortcode in versions up to, and including, 1.2. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes in the GBMI_Calc_Widget::widget() function. Shortcode attributes are extracted directly into local variables via @extract($args) and then		More

2026-8883	echoed unescaped into an HTML style attribute (height/width) and HTML body context (title), allowing attribute-breakout payloads. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	Details
CVE-2026-8895	The kk blog card plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'blog-card' shortcode in all versions up to, and including, 1.3. This is due to insufficient input sanitization and output escaping on the shortcode's 'href' and 'type' attributes, which are concatenated directly into HTML attribute contexts in the shortcode callback registered in kk-blog-card-shortcode.php. 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-2026-8977	The WP GDPR Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ninja_gdpr_ajax_actions' AJAX action in versions up to, and including, 1.0.0. This is due to missing capability and nonce checks on the handleAjaxCalls() function, combined with insufficient input sanitization on the gdprConfig values and missing output escaping in the generateCSS() function which echoes stored configuration values directly into a <style> block rendered on wp_head. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2021-47982	WordPress Plugin WP-Paginate 2.1.3 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by manipulating the preset parameter. Attackers can submit POST requests to the plugin settings page with script payloads in the preset parameter that are stored and executed when administrators view the settings.	6.4	More Details
CVE-2026-10732	All versions of the package decompress are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) when extracting a ZIP archive containing two entries with the same path - the first being a symlink to an arbitrary target and the second being a regular file - the file content is written through the symlink to the target location outside the output directory. This is due to the microtask processing order that checks readlink for the second file before resolving symlink for the first file. An attacker can write arbitrary file on the host filesystem potentially leading to remote code execution by providing a specially crafted ZIP archive. **Note:** This bypasses all existing path traversal protections including preventWritingThroughSymlink, added as a part of the fix for [CVE-2020-12265] (https://security.snyk.io/vuln/SNYK-JS-DECOMPRESS-557358).	6.4	More Details
CVE-2026-41975	Permission management vulnerability in the network management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	6.3	More Details
CVE-2026-11529	A vulnerability was determined in designcomputer mysql-mcp-server up to 0.2.2. The impacted element is the function read_resource of the file src/mysql_mcp_server/server.py of the component mysql URI Handler. This manipulation of the argument uri_str causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.3.0 is sufficient to resolve this issue. Patch name: 080bef9a96d625ce0dfbde573a08b93497871981. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-11521	A security vulnerability has been detected in Mohammed-eid35 bank-management-system-springboot up to 7b9bcc65ad7df3db29af71aed9bb500e5f24d948. This affects an unknown part of the file src/main/java/com/alien/bank/management/system/controller/TransactionController.java of the component Transaction Endpoint. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-47909	Dreamweaver Desktop versions 21.7 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	6.3	More Details
CVE-2026-47910	Dreamweaver Desktop versions 21.7 and earlier are affected by an Incorrect Authorization vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	6.3	More Details
CVE-2026-39170	SemCms 5.0 is vulnerable to Cross Site Request Forgery (CSRF) via crafted POST request to /admin/semcms_user.php.	6.3	More Details
	A vulnerability was identified in Dolibarr ERP CRM up to 23.0.2. The impacted element is an unknown		

CVE-2026-11619	function of the file htdocs/core/filemanagerdol/connectors/php/config.inc.php of the component Legacy Filemanager. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. Upgrading to version 23.0.3 is sufficient to resolve this issue. The identifier of the patch is f1b2dd6481e22cacb561d29ffdcd3a50b618479d. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-44275	Dell/Alienware Purchased Apps, versions prior to 1.1.32.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write	6.3	More Details
CVE-2026-41116	Dell Inventory Collector Client, versions prior to 13.8.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write.	6.3	More Details
CVE-2026-11585	A vulnerability was determined in CodeAstro Student Attendance Management System 1.0. Affected is an unknown function of the file /attendance-php/Admin/createClassArms.php. This manipulation of the argument classId causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-11584	A vulnerability was found in CodeAstro Student Attendance Management System 1.0. This impacts an unknown function of the file /attendance-php/Admin/createClass.php?action=edit. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-11583	A vulnerability has been found in CodeAstro Student Attendance Management System 1.0. This affects an unknown function of the file /attendance-php/Admin/createClass.php. The manipulation of the argument className leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-11559	A vulnerability was detected in CodeAstro Payroll System 1.0. This affects an unknown function of the file /view_account.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	6.3	More Details
CVE-2026-11558	A security vulnerability has been detected in CodeAstro Payroll System 1.0. The impacted element is an unknown function of the file /home_salary.php. The manipulation of the argument rate/salary_rate leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-11532	A weakness has been identified in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. Affected is an unknown function of the file /add.php of the component Student Record Handler. Executing a manipulation can lead to improper access controls. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11519	A security flaw has been discovered in SourceCodester Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /Product_Inventory/api/users_handler.php of the component Account Creation Handler. The manipulation of the argument ROLE results in improper authorization. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-10690	A vulnerability was identified in wonderwhy-er DesktopCommanderMCP 0.2.37. This affects the function readFileFromUrl of the file src/tools/filesystem.ts of the component read_file. Such manipulation of the argument url leads to server-side request forgery. The attack may be performed from remote. The exploit is publicly available and might be used. The name of the patch is 53699bebba9950047bca16ac4dc8f0568f596aaa. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-11495	A vulnerability was detected in CodeAstro Ingredients Stock Management System 1.0. This impacts an unknown function of the file /Ingredients-Stock/add_stock.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-11406	A vulnerability was determined in GL.iNet MT3000 up to 4.4.5. This vulnerability affects unknown code of the file ovpnclient.sh of the component OpenVPN Client Import Workflow. This manipulation causes command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. Upgrading to version 4.9.0_beta3-1012-0513-1778656146 is able to resolve this issue. You should upgrade the affected component. The vendor confirms: "This issue has been addressed by implementing malicious checks on OpenVPN configuration files to prevent command injection attacks carried through malicious configuration files."	6.3	More Details

CVE-2026-10815	A vulnerability was found in LakshayD02 Hostel-Management-System-PHP up to f87e67c283bab6f718faf2fec6ae39a13bd7036b. This issue affects some unknown processing of the file hostel/index.php of the component Admin Dashboard Page. The manipulation of the argument ID results in missing authorization. The attack can be launched remotely. The exploit has been made public and could be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2025-65640	Cross Site Scripting (XSS) vulnerability in the "Task in Progress / Recent" page in Arket Globe Document Intelligence 5.0.0.559 due to improper sanitization of user input in text fields when creating a new document. Specifically, when an authenticated attacker submits data containing JavaScript code within these fields, the application fails to properly sanitize or escape the content. As a result, the injected script is executed when the page is rendered, allowing the attacker to execute arbitrary JavaScript in the context of other users' browsers who view the affected page.	6.3	More Details
CVE-2026-21404	NAVTOR NavBox through version 4.16.1.20 contains hard-coded credentials within its Windows Communication Foundation (SOAP) implementation. If the SOAP functionality is enabled, a local attacker can extract credentials to bypass the intended transfer workflow. Successful authentication against the SOAP interface grants access to privileged WCF methods, enabling an attacker to write or overwrite files within application-defined paths.	6.3	More Details
CVE-2026-5589	An integer underflow in bt_mesh_sol_recv() in the Bluetooth Mesh solicitation handling (subsys/bluetooth/mesh/solicitation.c) leads to an out-of-bounds write. When CONFIG_BT_MESH_OD_PRIV_PROXY_SRV is enabled, the function parses solicitation PDUs from raw BLE advertising payloads. The AD parsing loop reads an attacker-controlled length byte (reported_len) and computes reported_len - 3 without checking that reported_len >= 3. When reported_len is less than 3, the subtraction is performed in signed int arithmetic and yields a negative value that bypasses the length guard and is then implicitly converted to a very large size_t when passed to net_buf_simple_pull_mem(). In builds without assertions, this wraps the buffer length and advances the data pointer far out of bounds, so subsequent reads dereference invalid memory. A nearby BLE device can trigger this with a non-connectable advertisement carrying a UUID16 AD structure and a crafted length byte, with no pairing or prior association required, potentially leading to denial of service or arbitrary code execution.	6.3	More Details
CVE-2026-42538	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 do not properly validate uploaded files. The application can therefore be misused to host phishing pages, amongst other things. This also creates another instance of a Cross-Site Scripting (XSS) vulnerability. Version 2.4.28 contains a patch.	6.3	More Details
CVE-2026-5066	A potential out-of-bounds write/read exists in the TLS socket connect path of the network sockets subsystem (subsys/net/lib/sockets/sockets_tls.c). When the TLS session cache is enabled, tls_session_store() and tls_session_restore() memcpy the caller-supplied address into a fixed-size buffer using the caller-controlled addrlen value without validating it against the destination size. struct net_sockaddr is an opaque type, so an application can pass an addrlen larger than sizeof(struct net_sockaddr) (for example 128 bytes into a 24-byte stack buffer), causing the memcpy to read and write past the end of the address memory used by the TLS session cache. This out-of-bounds write can lead to a crash and denial of service, and potentially to arbitrary code execution.	6.3	More Details
CVE-2026-10874	A vulnerability was identified in projectworlds Online Art Gallery Shop Project 1.0. The affected element is an unknown function of the file /admin/adminHome.php. The manipulation of the argument social_insta leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-10875	A security flaw has been discovered in projectworlds Online Art Gallery Shop Project 1.0. The impacted element is an unknown function of the file /admin/adminHome.ph. The manipulation of the argument social_twitter results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-10806	A vulnerability was found in mjperpinosa stumasy. The affected element is an unknown function of the file application/PHP/objects/updates/add_post.php. Performing a manipulation of the argument up_file_to_post results in unrestricted upload. The attack may be initiated remotely. The exploit has been made public and could be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11181	Inappropriate implementation in Media Session in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.3	More Details
CVE-	Insufficient policy enforcement in Actor in Google Chrome prior to 149.0.7827.53 allowed a remote		More

2026-11184	attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.3	Details
CVE-2026-11480	A vulnerability was found in Chengdu Everbrite Network Technology BeikeShop up to 1.6.0.22. Impacted is an unknown function of the file beike/Admin/Routes/admin.php of the component Admin Design Builder Endpoint. Performing a manipulation of the argument settings.value results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The patch is named 2fa9805411088069fcc3b0c15b2f1f33d6e09958. To fix this issue, it is recommended to deploy a patch.	6.3	More Details
CVE-2026-11187	Inappropriate implementation in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.3	More Details
CVE-2026-10876	A weakness has been identified in SourceCodester Ship Ferry Ticket Reservation System 1.0. This affects an unknown function of the file /admin/. This manipulation of the argument page causes improper authorization. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-10878	A vulnerability was detected in D-Link DWR-M920 1.1.50/1.1.70. Affected is the function sub_41C8E8 of the file /boafrm/formSmsManage. Performing a manipulation of the argument action_value results in command injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-10811	A security vulnerability has been detected in itsourcecode Fees Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /receipt.php. Such manipulation of the argument ef_id leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-11408	A vulnerability was identified in vertex-app vertex up to 2026.02.12. This issue affects some unknown processing of the file app/model/LogMod.js of the component Log Viewer Endpoint. Such manipulation of the argument req.query leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The name of the patch is 805d82e7100d49b79b3beb1b9420e8e458987198. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-39107	A Cross Site Scripting vulnerability exists in the Kimi AI v1.0 web interface's 'Preview' feature. The application fails to properly sanitize or encode HTML/JavaScript payloads generated by the AI model. When a user switches to the 'Preview' tab to view AI-generated code, the malicious payload is rendered directly into the DOM, leading to arbitrary JavaScript execution in the victim's browser session.	6.3	More Details
CVE-2026-11412	A weakness has been identified in Jinher OA C6. The affected element is an unknown function of the file /C6/JHSoft.Web.ModuleCount/GetFormSn.aspx. Executing a manipulation of the argument queryID can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-11473	A vulnerability was identified in jflyfox jfinal_cms up to 5.1.0. This impacts the function list of the file AdvicefeedbackController.java. Such manipulation of the argument orderBy leads to sql injection. The attack can be launched remotely. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11476	A security vulnerability has been detected in Kushan2k student-management-system up to f16a4ceaddd6729c4b306ed4641cda3176c1ef2a. Affected by this issue is the function edit-admin of the file controllers/AdminController.php of the component Profile Update Endpoint. The manipulation of the argument isadmin leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11470	A vulnerability has been found in hs-web hsweb-framework up to 5.0.1. The affected element is the function denied of the file hsweb-system/hsweb-system-file/src/main/java/org/hswebframework/web/file/FileUploadProperties.java of the component File Upload. The manipulation of the argument filename leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 8009845b577d8a2c4bbf4fdd8e8913799a714be6. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-11461	A vulnerability has been found in NousResearch hermes-agent up to 0.12.0. This affects the function resolve_session_by_title of the file hermes_state.py of the component resume Endpoint. Such manipulation of the argument Title leads to authorization bypass. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early	6.3	More Details

	about this disclosure but did not respond in any way.		
CVE-2026-11339	A vulnerability was detected in D-Link DWR-M920 up to 1.1.50. The affected element is the function sub_41CF20 of the file /boafrm/formUSSDSetup. The manipulation of the argument ussdValue results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-11453	A vulnerability was found in Tiobon Employee Self-Service System up to 7.2. Affected by this vulnerability is an unknown functionality of the file /Blog/BlogSearch.aspx of the component Login Endpoint. The manipulation of the argument Keyword results in sql 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-2026-11449	A security vulnerability has been detected in GL.iNet GL-MT3000 4.4.5. The impacted element is the function rpc_sys of the file /cgi-bin/luci/rpc of the component LuCI JSON-RPC Interface. Such manipulation leads to command injection. The attack may be performed from remote. Upgrading to version 4.8.1 is sufficient to resolve this issue. Upgrading the affected component is advised. The vendor confirms: "The issue discovered by the vulnerability researcher on older firmware versions(4.4.5) has actually been fixed and mitigated in the new version. According to the latest firmware fixes, by default, firmware versions after 4.7.13 do not install LuCI, so this vulnerability cannot be exploited."	6.3	More Details
CVE-2026-11447	A security flaw has been discovered in GL.iNet GL-MT3000 up to 4.4.5. Impacted is the function iwinfo_backend of the file iwinfo.so of the component MTK Backend. The manipulation of the argument device results in command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 4.7 is recommended to address this issue. Upgrading the affected component is recommended. The vendor confirms: "Starting from version 4.7, SDK has added global protection to intercept malicious injection".	6.3	More Details
CVE-2026-10807	A vulnerability was determined in mjperpinosa stumasy. The impacted element is an unknown function of the file application/PHP/objects/profiles/change_profile_image.php. Executing a manipulation of the argument pr_profile_image can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11441	A vulnerability was identified in theonedev onedev up to 15.0.5. This vulnerability affects the function canAccessIssue of the file /issues/ of the component Pull Request Handler. Such manipulation of the argument issue leads to improper authorization. It is possible to launch the attack remotely. Upgrading to version 15.0.6 is able to resolve this issue. It is advisable to upgrade the affected component.	6.3	More Details
CVE-2026-11440	A vulnerability was determined in theonedev onedev up to 15.0.5. This affects an unknown part of the file /repositories/{projectId}/default-branch of the component REST API. This manipulation of the argument project.defaultBranch causes improper authorization. It is possible to initiate the attack remotely. Upgrading to version 15.0.6 is able to mitigate this issue. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-11439	A vulnerability was found in theonedev onedev up to 15.0.5. Affected by this issue is some unknown functionality of the file /projects/ of the component Parent Project Handler. The manipulation of the argument project.parentId results in improper authorization. The attack may be performed from remote. Upgrading to version 15.0.6 can resolve this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-11438	A vulnerability has been found in theonedev onedev up to 15.0.5. Affected by this vulnerability is an unknown functionality of the file /projects. The manipulation of the argument project.forkedFromId leads to improper authorization. The attack is possible to be carried out remotely. Upgrading to version 15.0.6 addresses this issue. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-10808	A vulnerability was identified in itsourcecode Fees Management System 1.0. This affects an unknown function of the file /manage_student.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-10809	A security flaw has been discovered in itsourcecode Fees Management System 1.0. This impacts an unknown function of the file /manage_user.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-11308	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Low)	6.3	More Details
	A weakness has been identified in Kushan2k student-management-system up to		

CVE-2026-11475	f16a4ceaddd6729c4b306ed4641cda3176c1ef2a. Affected by this vulnerability is the function getStatus of the file controllers/GradeController.php of the component Certificate Verification Endpoint. Executing a manipulation of the argument nic can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11513	A vulnerability was detected in itsourcecode Hospital Management System 1.0. Impacted is an unknown function of the file /adminaccount.php. The manipulation of the argument Date results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-11514	A flaw has been found in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /addpatient.php. This manipulation of the argument admissiontme causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-11507	A vulnerability was found in CodeAstro Leave Management System 1.0. Affected is an unknown function of the file /admin/delete_leave_type.php. The manipulation of the argument leave_type results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-11508	A vulnerability was determined in CodeAstro Leave Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/search_staff_to_assign_pc.php. This manipulation of the argument Name causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-11509	A vulnerability was identified in CodeAstro Leave Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/search_staff_for_updation.php. Such manipulation of the argument Name leads to sql injection. The attack may be performed from remote.	6.3	More Details
CVE-2026-11510	A security flaw has been discovered in CodeAstro Leave Management System 1.0. This affects an unknown part of the file /admin/add_leave.php. Performing a manipulation of the argument type_of_leave results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-11333	A security vulnerability has been detected in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. The impacted element is an unknown function of the file dashboard_page/forms/upload_student_data.php of the component Student Data Upload Endpoint. Such manipulation of the argument Student-Data-CSV leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11335	A flaw has been found in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. This impacts the function session_start of the file /login-form.php. Executing a manipulation of the argument UserAuthData can lead to session fixiation. The attack can be launched remotely. The exploit has been published and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-11506	A vulnerability has been found in CodeAstro Leave Management System 1.0. This impacts an unknown function of the file /admin/search_staff_for_deletion.php. The manipulation of the argument Name leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-10693	A security vulnerability has been detected in SourceCodester Online Boat Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the component Administrative Endpoint. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Multiple endpoints are affected.	6.3	More Details
CVE-2026-10703	A security vulnerability has been detected in EIPStackGroup OpENer up to 2.3.0. Affected is the function CreateMessageRouterRequestStructure of the file cipmessagerouter.c of the component SendRRData Handler. The manipulation leads to use after free. Remote exploitation of the attack is possible. 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.	6.3	More Details
CVE-2026-11341	A flaw has been found in D-Link DWR-M920 up to 1.1.50. The impacted element is the function sub_412DA0 of the file /boafrm/formIMEISetup. This manipulation of the argument IMEI_value causes os command injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details

CVE-2026-11336	A vulnerability has been found in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. Affected is an unknown function of the file dashboard_page/admin_page.php of the component Admin Interface. The manipulation of the argument UserAuthData leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2016-20064	WP Vault 0.8.6.6 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting an unescaped parameter in the include functionality. Attackers can supply directory traversal sequences through the wpv-image GET parameter to access sensitive files like system configuration and credentials.	6.2	More Details
CVE-2026-47903	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Input Validation vulnerability. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	6.2	More Details
CVE-2023-43686	An issue was discovered in Malwarebytes 4.x and 5.x (and Nebula 2020-10-21 and later). A large number of Firefox preference files can cause the parser to ignore other browser configuration files, leading to a denial of service.	6.2	More Details
CVE-2022-50953	WordPress Plugin admin-word-count-column 2.2 contains a local file read vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting null byte injection in the path parameter. Attackers can send GET requests to download-csv.php with a crafted path parameter containing directory traversal sequences and null bytes to bypass file restrictions and read sensitive files like system configuration.	6.2	More Details
CVE-2026-47904	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	6.2	More Details
CVE-2026-42771	Issue summary: When the X509_VERIFY_PARAM_set1_email is called by an application to validate a crafted e-mail address, such as during S/MIME message validation, an out of bounds read can happen. Impact summary: This out of bounds read will not directly exfiltrate the data read to the attacker so the most likely result is a crash and a Denial of Service. An internal helper function called from X509_VERIFY_PARAM_[set|add]_email() used a wrong length when validating the local part of an email address. This could cause the 64 octet limit on the local part of an email address to be not enforced, or cause an out of bound read and potentially a crash. The bug is reachable via S-MIME validation with a crafted From: address supplied in an email message that can potentially cause a crash. No FIPS modules are affected by this issue as the affected code is outside the OpenSSL FIPS module boundary.	6.2	More Details
CVE-2026-45491	Improper link resolution before file access ('link following') in .NET allows an unauthorized attacker to perform tampering locally.	6.2	More Details
CVE-2026-47902	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	6.2	More Details
CVE-2026-47905	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	6.2	More Details
CVE-2026-45500	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	6.1	More Details
CVE-2026-10916	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	6.1	More Details
CVE-2026-8910	The WP Emoticon Rating plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details

CVE-2026-11034	Insufficient validation of untrusted input in Tab Group Sync in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via malicious network traffic. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-11122	Inappropriate implementation in Keyboard in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-11150	Inappropriate implementation in XML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-9280	The Ad Inserter – Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL Parameters in iframe Mode in all versions up to, and including, 2.8.15 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. Exploitation requires that iframe mode (AI_OPTION_IFRAME) is enabled on at least one ad block displayed on the targeted page, which is a non-default but supported configuration commonly used for AdSense and JavaScript-based ads.	6.1	More Details
CVE-2026-29170	A cross-site scripting vulnerability exists in mod_proxy_ftp's HTML directory list generation in Apache HTTP Server 2.4.67 and earlier when listing FTP directory contents either via forward or reverse proxy configuration. Users are recommended to upgrade to version 2.4.68, which fixes this issue.	6.1	More Details
CVE-2026-10861	An open redirect vulnerability existed in MISP UsersController::routeafterlogin() because the value stored in the pre_login_requested_url session key was used as the post-login redirect destination without sufficiently enforcing that it was a local application path. An unauthenticated remote attacker could craft a link that causes a victim to visit a trusted MISP instance and, after successful authentication, be redirected to an attacker-controlled external URL. This could be abused to increase the credibility of phishing attacks, redirect users to counterfeit login pages, or deliver attacker-controlled content from an untrusted domain. CWE-601 describes this weakness as accepting user-controlled input that specifies an external link and using it in a redirect, with phishing as a common consequence. The patch mitigates the issue by decoding and parsing the URL, rejecting URLs with a scheme, host, user component, missing or non-local path, and protocol-relative forms such as //example.com and /\example.com.	6.1	More Details
CVE-2026-10856	A URL validation flaw in the MISP dashboard button widget allowed a crafted relative-looking URL to be accepted as a local path while being interpreted by browsers as an external URL. The validation rejected URLs containing an explicit scheme, host, or user component, but did not reject paths beginning with a slash followed by a backslash, such as /\example.com. Some browsers normalize backslashes in URLs as forward slashes, which can turn this into a scheme-relative external navigation target. In addition, the generated href concatenated the reconstructed URL with the original URL, increasing the possibility of unsafe or malformed link generation. An attacker able to configure or influence a dashboard button URL could craft a button that appears to point inside the application but redirects users to an attacker-controlled site when clicked. This could be used for phishing, credential theft, or social engineering. The patch fixes the issue by rejecting empty paths and paths starting with /\, and by emitting only the reconstructed validated URL in the anchor href.	6.1	More Details
CVE-2025-40808	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions), SIPROTEC 5 6MD89 (CP300) (All versions), SIPROTEC 5 6MU85 (CP300) (All versions), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions), SIPROTEC 5 7SJ81 (CP100) (All versions), SIPROTEC 5 7SJ81 (CP150) (All versions), SIPROTEC 5 7SJ82 (CP100) (All versions), SIPROTEC 5 7SJ82 (CP150) (All versions), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions), SIPROTEC 5 7SK82 (CP100) (All versions), SIPROTEC 5 7SK82 (CP150) (All versions), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions), SIPROTEC 5 7ST86 (CP300) (All versions), SIPROTEC 5 7SX82 (CP150) (All versions), SIPROTEC 5 7SX85 (CP300) (All versions), SIPROTEC 5 7SY82 (CP150) (All versions), SIPROTEC 5 7UM85 (CP300) (All versions), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions), SIPROTEC	6.1	More Details

	5 7VE85 (CP300) (All versions), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions), SIPROTEC 5 7VU85 (CP300) (All versions), SIPROTEC 5 Compact 7SX800 (CP050) (All versions). The affected application allows authenticated users to upload arbitrary files using DIGSI 5 protocol. This could allow an attacker to upload malicious configuration files, that could cause denial of service condition and potentially lead to code execution.		
CVE-2026-25699	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. Timeline-related APIs lacked proper authorization checks, allowing regular authenticated users to access deleted, private, or unapproved content and its revision history. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	6.1	More Details
CVE-2026-25860	OpenClinic GA 5.351.19 contains a reflected cross-site scripting vulnerability in the DICOM image upload handler that allows attackers to execute arbitrary JavaScript in a victim's browser by embedding malicious payloads in DICOM file metadata fields. Attackers can craft a DICOM file with JavaScript payloads in metadata fields such as Study Description, which are reflected without sanitization in popup.jsp and archiving/uploadfiles_jsp.java when processed through the Upload DICOM images feature.	6.1	More Details
CVE-2026-34417	OSCAL-GUI contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser by injecting malicious content through the project request parameter in oscal-forms.php. The parameter value is URL-decoded and assigned to the project_id variable without sanitization in oscal-functions.php, and when the supplied project ID is not found, the unsanitized value is concatenated into an error message via the Messages() function and reflected into the HTML response body without encoding.	6.1	More Details
CVE-2026-25688	Improper Neutralization of Alternate XSS Syntax vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. AI-generated response content was rendered in the browser without proper sanitization, allowing malicious scripts to be executed when the content was viewed. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	6.1	More Details
CVE-2026-38579	Multiple reflected Cross-Site Scripting (XSS) vulnerabilities in damasac thaipalliative_lte through version 3.0 allow remote attackers to inject arbitrary web script or HTML via the idFormMain parameter (line 24), the id parameter (lines 25, 75), and the ptid_key parameter (lines 26, 42) in /substudy/ezform.php. User input is echoed into HTML attributes and JavaScript contexts without encoding.	6.1	More Details
CVE-2026-50235	Lyrion Music Server 9.2.0 contains a reflected cross-site scripting vulnerability in advanced search parameters that fail to properly sanitize user input before displaying it in search forms. Attackers can inject malicious scripts through unfiltered search parameters to execute arbitrary JavaScript in users' browsers and steal session information.	6.1	More Details
CVE-2026-8907	The WP-Ultimate-Map plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1. This is due to missing nonce validation on the process_init() function hooked to admin_init, which saves plugin settings (zoom-level, focus-lat, focus-lng, sel_places, sel_routes) via update_option() based solely on the presence of a save-setting POST parameter. Additionally, the saved values — particularly zoom-level — are stored without sanitization and later echoed into an HTML attribute (and inline JavaScript) on the settings page without escaping. This makes it possible for unauthenticated attackers to change plugin settings and inject arbitrary web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-8916	Out-of-bounds write vulnerability in Samsung Open Source rlottie allows Overflow Buffers. This issue affects rlottie: before dcfde72eae1b0464dc0dd760aec00ada6a148635.	6.1	More Details
CVE-2026-11205	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted QR code. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-41715	In specific scenarios involving HTTP redirects from a secure to an insecure endpoint, the Reactor Netty HTTP client may leak credentials. In order for this to happen, the HTTP client must have been explicitly configured to follow redirects. Affected versions: Reactor Netty 1.0.0 through 1.0.51; 1.1.0 through 1.1.35; 1.2.0 through 1.2.17; 1.3.0 through 1.3.5.	6.1	More Details
CVE-2026-32856	Ellucian Banner Self-Service before the April T2 release (2025-04-23) contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser by injecting unsanitized input through the toDateFormat request parameter in the dateConverter endpoint. Attackers can craft a malicious URL targeting the unauthenticated dateConverter endpoint to steal session cookies or perform other malicious actions in the context of the victim's browser session.	6.1	More Details
CVE-	The Product Filter Widget for Elementor plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 'args[filterFormArray]' Parameter in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject		More

2026-11603	arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The endpoint is registered via wp_ajax_nopriv_ with no nonce verification or capability check, and exploitation is delivered via a CSRF-style form auto-submission to the admin-ajax.php endpoint, requiring the attacker to trick a victim into visiting an attacker-controlled page.	6.1	Details
CVE-2026-21826	HCL Digital Experience and HCL Digital Experience Compose could be susceptible to Host header injection. An attacker can manipulate the Host header and cause the application to behave in unexpected ways.	6.1	More Details
CVE-2026-21825	HCL Digital Experience Compose is affected by a reflected cross-site scripting (XSS) vulnerability in the search center. An attacker could execute arbitrary JavaScript in the victim's browser.	6.1	More Details
CVE-2026-11273	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Low)	6.1	More Details
CVE-2026-44746	Due to a reflected cross-site scripting (XSS) vulnerability in SAP NetWeaver JAVA (JDBC Test Servlet), an unauthenticated attacker could craft a URL that embeds a malicious script. If a victim clicks this link, the injected input is processed during web page generation, resulting in the execution of malicious content in the victim's browser. This could allow the attacker to access and/or modify information related to the webclient, impacting the confidentiality and integrity of the application, with no impact to availability.	6.1	More Details
CVE-2026-49510	Integer overflow or wraparound vulnerability in Samsung Open Source rlottie allows Integer Attacks. This issue affects rlottie: before 21292665023e5074b38254432716866d00f1985f.	6.1	More Details
CVE-2026-50230	Lyrion Music Server 9.2.0 contains an unauthenticated reflected cross-site scripting vulnerability in the server.log endpoint that allows attackers to inject arbitrary HTML and JavaScript code through the search parameter. Attackers can craft malicious URLs with JavaScript payloads in the search parameter to execute code in users' browsers within the context of the affected application.	6.1	More Details
CVE-2026-11229	Inappropriate implementation in Enterprise in Google Chrome prior to 149.0.7827.53 allowed a local attacker to perform privilege escalation via physical access to the device. (Chromium security severity: Low)	6.1	More Details
CVE-2026-36725	A markdown based cross-site scripting (XSS) vulnerability in the /system/notice/create endpoint of FastapiAdmin v2.2.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the notice_content parameter.	6.1	More Details
CVE-2026-47306	Uncontrolled Recursion vulnerability in Samsung Open Source rlottie allows Oversized Serialized Data Payloads. This issue affects rlottie: before e2d19e3b150e0e4a9586fa90b56fd3061cc98945.	6.1	More Details
CVE-2026-34416	OSCAL-GUI contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser by injecting malicious input through the project request parameter. Attackers can craft a malicious URL containing unsanitized input that breaks out of the JavaScript string and HTML attribute context in the body onload event handler to execute arbitrary scripts when the link is visited by a victim.	6.1	More Details
CVE-2026-47320	Access of uninitialized pointer, Uncontrolled Recursion vulnerability in Samsung Open Source rlottie allows Pointer Manipulation, Oversized Serialized Data Payloads. This issue affects rlottie: before eae37633fda13ac05b25c6c95aacea4bc33c80a3.	6.1	More Details
CVE-2026-47318	Stack-based buffer overflow vulnerability in Samsung Open Source rlottie allows Overflow Buffers. This issue affects rlottie: before ce72b35a7ad0dded03051d3aa0ef75321c3bd035.	6.1	More Details
CVE-2026-20233	A vulnerability in the web-based user interface of Cisco Webex Meetings could have allowed an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. Cisco has addressed this vulnerability in the Webex Meetings service, and no customer action is needed. This vulnerability existed because of insufficient validation of user input. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful exploit could have allowed the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.	6.1	More Details
CVE-2026-47319	Memory allocation with excessive size value vulnerability in Samsung Open Source rlottie allows Excessive Allocation. This issue affects rlottie: before 0b4e308fa88c72cbb60cc8a2c1d2c2ad89b101dd.	6.1	More Details
	A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to load arbitrary files		

CVE-2026-20175	from remote locations into an active user session on an affected device, possibly leading to browser-based attacks. This vulnerability is due to insufficient validation of user-supplied input for HTTP requests that are sent to an affected device. An attacker who has knowledge of the address of the affected device could exploit this vulnerability by persuading a user to click a crafted link that contains the affected device address. A successful exploit could allow the attacker to conduct browser-based attacks and execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device.	6.1	More Details
CVE-2026-10305	Out-of-bounds read vulnerability in Samsung Open Source rlottie allows Overread Buffers. This issue affects rlottie: before 223a2a41ba4f462e4abe767bebba49a366c9b9fd.	6.1	More Details
CVE-2026-11186	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	6.1	More Details
CVE-2026-25622	A Captive Portal Custom Handler command injection vulnerability exists in Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). On affected platforms, an administrative account logged into the user interface can exploit this input handling behavior to execute arbitrary platform shell commands.	6.0	More Details
CVE-2026-25620	An encrypted password command injection vulnerability exists in the Captive Portal application framework of Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). This issue uniquely affects version 17.4.0; earlier software releases are not exposed.	6.0	More Details
CVE-2026-25621	A Reports application infrastructure vulnerability exists in Arista Edge Threat Management - Arista Next Generation Firewall (NGFW) due to insecure input validation. This issue uniquely affects version 17.4.0; earlier software releases are not exposed.	6.0	More Details
CVE-2026-25623	An input validation command execution vulnerability exists in the browser management pipeline of Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). Authenticated administrators can leverage this exposure to obtain underlying terminal script code processing execution permissions.	6.0	More Details
CVE-2026-28262	Dell iDRAC Tools, versions prior to 11.4.1.0, contains an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	6.0	More Details
CVE-2026-41973	Permission control vulnerability in calls. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2026-11788	A flaw was found in 389 Directory Server. The dereference control plugin does not check for allocation failure before using a BER structure, allowing an unauthenticated remote attacker to crash the LDAP server when the system is under memory pressure.	5.9	More Details
CVE-2026-41710	An attacker can craft a large number of unique requests that trigger a failure, exhausting the capacity of the application-wide stateful retry cache. Once the cache is full, it permanently rejects any further updates, causing all later stateful retries and circuit breakers in the application to fail. Affected versions: Spring Retry 2.0.0 through 2.0.12; 1.3.0 through 1.3.4.	5.9	More Details
CVE-2026-41846	Spring MVC applications which accept user-supplied values in the cssClass, cssErrorClass, or cssStyle attributes of JSP form tags allow arbitrary HTML/JavaScript code injection, potentially resulting in a cross-site scripting (XSS) vulnerability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	5.9	More Details
CVE-2026-41841	Spring MVC and WebFlux applications are vulnerable to Information Disclosure attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	5.9	More Details
CVE-2026-42766	Issue summary: A specially crafted password-encrypted CMS message can trigger a NULL pointer dereference during CMS decryption. Impact summary: This NULL pointer dereference leads to an application crash and a Denial of Service. The CMS PasswordRecipientInfo.keyDerivationAlgorithm field is defined as OPTIONAL in the ASN.1 specification and may therefore be absent in specially crafted inputs. During the password-based CMS decryption the OpenSSL CMS implementation dereferences this field without first checking whether it was present. An attacker who supplies such a CMS message to an application performing password-based CMS decryption can trigger an application crash, leading to a Denial of Service. Applications that process password-encrypted CMS messages may be affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	5.9	More Details
CVE-	Inappropriate implementation in WebRTC in Google Chrome prior to 149.0.7827.53 allowed an attacker in		More

2026-11199	a privileged network position to leak cross-origin data via malicious network traffic. (Chromium security severity: Medium)	5.9	Details
CVE-2026-11238	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. (Chromium security severity: Low)	5.9	More Details
CVE-2023-5502	On affected platforms running Arista EOS with 802.1x authentication configured on the access/trunk ports, and routing enabled on the access VLAN of the ports, a malicious supplicant may be able to bypass the requirement to perform 802.1x authentication.	5.9	More Details
CVE-2026-2379	On affected platforms with hardware IPSec support running Arista EOS with certain IPsec features enabled, EOS may exhibit unexpected behavior in specific cases. Physical interface flaps and certain agent restarts can cause IPsec tunnel re-establishment with existing Security Associations, resulting in sequence number mismatches between tunnel endpoints potentially causing unstable communication.	5.9	More Details
CVE-2026-41843	Spring MVC and WebFlux applications are vulnerable to Path Traversal attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	5.9	More Details
CVE-2026-41840	Spring WebFlux applications are vulnerable to Denial of Service (DoS) attacks when processing multipart requests. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	5.9	More Details
CVE-2026-42767	Issue summary: An attacker-controlled CMP (Certificate Management Protocol) server could trigger a NULL pointer dereference in a CMP client application. Impact summary: A NULL pointer dereference causes a crash of the application and a Denial of Service. An attacker controlling a CMP server (or acting as a man-in-the-middle) could craft a CMP response containing a CRMF (Certificate Request Message Format) CertRepMessage with an EncryptedValue structure where the symmAlg field has an algorithm OID but no parameters field. When the OpenSSL CMP client processes this response, the NULL dereference occurs, causing a crash of the CMP client. Applications that process untrusted CMP/CRMF messages may be affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	5.9	More Details
CVE-2026-36616	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 contains hardcoded WiFi driver credentials including a RADIUS shared secret, WPS test key, and default PSK embedded in the production firmware binary.	5.9	More Details
CVE-2026-34694	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.9	More Details
CVE-2026-36610	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 transmits DDNS credentials over plaintext HTTP with only Base64 encoding. The firmware contains no TLS implementation, allowing man-in-the-middle interception of DDNS service credentials.	5.9	More Details
CVE-2026-48681	OpenStack Ironic through before 35.0.2 allows file overwrite via directory traversal during deployment with a crafted ISO image.	5.9	More Details
CVE-2023-52951	A cleartext transmission of sensitive information vulnerability in Synology Note Station Client before 2.2.4-703 allows man-in-the-middle attackers to obtain user credential.	5.9	More Details
CVE-2026-46447	OpenStack Ironic before 35.0.2 allows Boot Script Injection of an iPXE script if the attacker can set node.driver_info or node.instance_info.	5.8	More Details
CVE-2026-7473	On affected platforms running Arista EOS where a tunnel decapsulation configuration—such as VXLAN (Virtual Extensible LAN), decap-groups, or a GRE (Generic Routing Encapsulation) tunnel interface—is present, the switch will incorrectly decapsulate and forward other unexpected tunneled packet with a destination IP matching its configured decapsulation IP. This occurs because the switch does not verify the tunnel protocol type, potentially leading to the unexpected processing of non-configured tunnel traffic. This issue has been reported as being exploited in the wild.	5.8	More Details
CVE-2026-40639	Dell Client Platform BIOS contains a Weak Encoding for Password vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Elevation of Privileges.	5.7	More Details
	An administrative cross-site scripting (XSS) vulnerability exists in the web user interface dashboard layout		

CVE-2026-25624	of Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). Unvalidated user-supplied variables are echoed back to administrative profiles, facilitating vector payload processing behavior controls.	5.7	More Details
CVE-2026-42915	Incorrect calculation of buffer size in Windows TCP/IP allows an authorized attacker to deny service over an adjacent network.	5.7	More Details
CVE-2026-6899	Check for certificate revocation only considers the first matching CRL and ignores other valid CRLs of the same CA in the CycloneCrypto cryptographic wrapper of S2OPC library. It might allow connection between an OPC UA client and server using a revoked certificate.	5.6	More Details
CVE-2026-46261	In the Linux kernel, the following vulnerability has been resolved: spi: wpcm-fiu: Fix potential NULL pointer dereference in wpcm_fiu_probe() platform_get_resource_byname() can return NULL, which would cause a crash when passed the pointer to resource_size(). Move the fiu->memory_size assignment after the error check for devm_ioremap_resource() to prevent the potential NULL pointer dereference.	5.5	More Details
CVE-2026-46268	In the Linux kernel, the following vulnerability has been resolved: PCI/P2PDMA: Fix p2pmem_alloc_mmap() warning condition Commit b7e282378773 has already changed the initial page refcount of p2pdma page from one to zero, however, in p2pmem_alloc_mmap() it uses "VM_WARN_ON_ONCE_PAGE(!page_ref_count(page))" to assert the initial page refcount should not be zero and the following will be reported when CONFIG_DEBUG_VM is enabled: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x380400000 flags: 0x20000000002000(reserved|node=0|zone=4) raw: 0020000000002000 ff1100015e3ab440 0000000000000000 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: VM_WARN_ON_ONCE_PAGE(!page_ref_count(page)) ----------[cut here]---------- WARNING: CPU: 5 PID: 449 at drivers/pci/p2pdma.c:240 p2pmem_alloc_mmap+0x83a/0xa60 Fix by using "page_ref_count(page)" as the assertion condition.	5.5	More Details
CVE-2026-46262	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl_xcvr: Revert fix missing lock in fsl_xcvr_mode_put() This reverts commit f51424872760 ("ASoC: fsl_xcvr: fix missing lock in fsl_xcvr_mode_put()"). The original patch attempted to acquire the card->controls_rwsem lock in fsl_xcvr_mode_put(). However, this function is called from the upper ALSA core function snd_ctl_elem_write(), which already holds the write lock on controls_rwsem for the whole put operation. So there is no need to simply hold the lock for fsl_xcvr_activate_ctl() again. Acquiring the read lock while holding the write lock in the same thread results in a deadlock and a hung task, as reported by Alexander Stein.	5.5	More Details
CVE-2026-45594	Exposure of sensitive information to an unauthorized actor in Windows Application Identity (AppID) Subsystem allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-46258	In the Linux kernel, the following vulnerability has been resolved: gpio: cdev: Avoid NULL dereference in linehandle_create() In linehandle_create(), there is a statement like this: retain_and_null_ptr(lh); Soon after, there is a debug printout that dereferences "lh", which will crash things. Avoid the crash by using handlereq.lines, which is the same value.	5.5	More Details
CVE-2026-45634	Out-of-bounds read in Windows DHCP Server allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-46257	In the Linux kernel, the following vulnerability has been resolved: clocksource/drivers/timer-sp804: Fix an Oops when read_current_timer is called on ARM32 platforms where the SP804 is not registered as the sched_clock. On SP804, the delay timer shares the same clkevt instance with sched_clock. On some platforms, when sp804_clocksource_and_sched_clock_init is called with use_sched_clock not set to 1, sched_clkevt is not properly initialized. However, sp804_register_delay_timer is invoked unconditionally, and read_current_timer() subsequently calls sp804_read on an uninitialized sched_clkevt, leading to a kernel Oops when accessing sched_clkevt->value. Declare a dedicated clkevt instance exclusively for delay timer, instead of sharing the same clkevt with sched_clock. This ensures that read_current_timer continues to work correctly regardless of whether SP804 is selected as the sched_clock.	5.5	More Details
CVE-2026-46256	In the Linux kernel, the following vulnerability has been resolved: NFS/localio: prevent direct reclaim recursion into NFS via nfs_writepages LOCALIO is an NFS loopback mount optimization that avoids using the network for READ, WRITE and COMMIT if the NFS client and server are determined to be on the same system. But because LOCALIO is still fundamentally "just NFS loopback mount" it is susceptible to recursion deadlock via direct reclaim, e.g.: NFS LOCALIO down to XFS and then back into NFS via nfs_writepages. Fix LOCALIO's potential for direct reclaim deadlock by ensuring that all its page cache allocations are done from GFP_NOFS context. Thanks to Ben Coddington for pointing out commit ad22c7a043c2 ("xfs: prevent stack overflows from page cache allocation").	5.5	More Details

CVE-2026-46255	In the Linux kernel, the following vulnerability has been resolved: dmaengine: fsl-edma: don't explicitly disable clocks in .remove() The clocks in fsl_edma_engine::muxclk are allocated and enabled with devm_clk_get_enabled(), which automatically cleans these resources up, but these clocks are also manually disabled in fsl_edma_remove(). This causes warnings on driver removal for each clock: edma_module already disabled WARNING: CPU: 0 PID: 418 at drivers/clk/clk.c:1200 clk_core_disable+0x198/0x1c8 [...] Call trace: clk_core_disable+0x198/0x1c8 (P) clk_disable+0x34/0x58 fsl_edma_remove+0x74/0xe8 [fsl_edma] [...] ---[end trace 0000000000000000]--- edma_module already unprepared WARNING: CPU: 0 PID: 418 at drivers/clk/clk.c:1059 clk_core_unprepare+0x1f8/0x220 [...] Call trace: clk_core_unprepare+0x1f8/0x220 (P) clk_unprepare+0x34/0x58 fsl_edma_remove+0x7c/0xe8 [fsl_edma] [...] ---[end trace 0000000000000000]--- Fix these warnings by removing the unnecessary fsl_disable_clocks() call in fsl_edma_remove().	5.5	More Details
CVE-2026-45604	Out-of-bounds read in Windows Application Identity (AppID) Subsystem allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-45606	Out-of-bounds read in Microsoft UxTheme Library (uxtheme.dll) allows an authorized attacker to deny service locally.	5.5	More Details
CVE-2026-45581	fabric-chaincode-java is a Java based implementation of Hyperledger Fabric chaincode shim APIs. From version 2.3.1 to before version 2.5.10, when chaincode is deployed in chaincode-as-a-service mode with TLS enabled, the chaincode server INFO level logging includes the TLS private key password in plaintext. An attacker with access to the chaincode server logs could recover the TLS private key password. If the attacker can also obtain the TLS private key, they could impersonate the chaincode server. This issue has been patched in version 2.5.10.	5.5	More Details
CVE-2026-46269	In the Linux kernel, the following vulnerability has been resolved: pinctrl: canaan: k230: Fix NULL pointer dereference when parsing devicetree When probing the k230 pinctrl driver, the kernel triggers a NULL pointer dereference. The crash trace showed: [0.732084] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000068 [0.740737] ... [0.776296] epc : k230_pinctrl_probe+0x1be/0x4fc In k230_pinctrl_parse_functions(), we attempt to retrieve the device pointer via info->pctl_dev->dev, but info->pctl_dev is only initialized after k230_pinctrl_parse_dt() completes. At the time of DT parsing, info->pctl_dev is still NULL, leading to the invalid dereference of info->pctl_dev->dev. Use the already available device pointer from platform_device instead of accessing through uninitialized pctl_dev.	5.5	More Details
CVE-2026-42906	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-34704	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-42968	Out-of-bounds read in Windows Telephony Service allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-42969	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-42970	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-42971	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-42972	Exposure of sensitive information to an unauthorized actor in Windows Hyper-V allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-42973	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	5.5	More Details

CVE-2026-44821	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2026-48566	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-34705	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-44814	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-34703	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-45647	Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Endpoint allows an authorized attacker to elevate privileges locally.	5.5	More Details
CVE-2026-44805	Use after free in Windows Network Controller (NC) Host Agent allows an authorized attacker to deny service locally.	5.5	More Details
CVE-2026-46254	In the Linux kernel, the following vulnerability has been resolved: AppArmor: Allow apparmor to handle unaligned dfa tables The dfa tables can originate from kernel or userspace and 8-byte alignment isn't always guaranteed and as such may trigger unaligned memory accesses on various architectures. Resulting in the following [73.901376] WARNING: CPU: 0 PID: 341 at security/apparmor/match.c:316 aa_dfa_unpack+0x6cc/0x720 [74.015867] Modules linked in: binfmt_misc evdev flash sg drm drm_panel_orientation_quirks backlight i2c_core configfs nfnetlink autofs4 ext4 crc16 mbcache jbd2 hid_generic usbhid sr_mod hid cdrom sd_mod ata_generic ohci_pci ehci_pci ehci_hcd ohci_hcd pata_ali libata sym53c8xx scsi_transport_spi tg3 scsi_mod usbcore libphy scsi_common mdio_bus usb_common [74.428977] CPU: 0 UID: 0 PID: 341 Comm: apparmor_parser Not tainted 6.18.0-rc6+ #9 NONE [74.536543] Call Trace: [74.568561] [<0000000000434c24>] dump_stack+0x8/0x18 [74.633757] [<0000000000476438>] __warn+0xd8/0x100 [74.696664] [<00000000004296d4>] warn_slowpath_fmt+0x34/0x74 [74.771006] [<00000000008db28c>] aa_dfa_unpack+0x6cc/0x720 [74.843062] [<00000000008e643c>] unpack_pdb+0xbc/0x7e0 [74.910545] [<00000000008e7740>] unpack_profile+0xbe0/0x1300 [74.984888] [<00000000008e82e0>] aa_unpack+0xe0/0x6a0 [75.051226] [<00000000008e3ec4>] aa_replace_profiles+0x64/0x1160 [75.130144] [<00000000008d4d90>] policy_update+0xf0/0x280 [75.201057] [<00000000008d4fc8>] profile_replace+0xa8/0x100 [75.274258] [<0000000000766bd0>] vfs_write+0x90/0x420 [75.340594] [<00000000007670cc>] ksys_write+0x4c/0xe0 [75.406932] [<0000000000767174>] sys_write+0x14/0x40 [75.472126] [<0000000000406174>] linux_sparc_syscall+0x34/0x44 [75.548802] ---[end trace 0000000000000000]--- [75.609503] dfa blob stream 0xfff0000008926b96 not aligned. [75.682695] Kernel unaligned access at TPC[8db2a8] aa_dfa_unpack+0x6e8/0x720 Work around it by using the get_unaligned_xx() helpers.	5.5	More Details
CVE-2025-70100	A divide-by-zero vulnerability in the ext4_block_set_lb_size function in src/ext4_blockdev.c of the lwext4 1.0.0 library allows attackers to cause a denial of service by providing a malformed ext4 filesystem image that results in a zero logical block size. The vulnerability is triggered during mount or image processing and leads to a Floating-Point Exception (FPE) under sanitizers or a runtime crash in standard builds due to missing validation of lb_size.	5.5	More Details
CVE-2026-9735	MongoDB server may log authentication parameters, including credentials, to the server log during SASL authentication. When connection health metric logging is enabled, the full authentication parameters are written to the log without redaction.	5.5	More Details
CVE-2026-47961	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this		More

2026-47926	vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	Details
CVE-2026-47925	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-47924	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-47923	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-41979	Permission control vulnerability in the print module. Impact: Successful exploitation of this vulnerability may affect integrity and confidentiality.	5.5	More Details
CVE-2026-46252	In the Linux kernel, the following vulnerability has been resolved: regulator: core: fix locking in regulator_resolve_supply() error path If late enabling of a supply regulator fails in regulator_resolve_supply(), the code currently triggers a lockdep warning: WARNING: drivers/regulator/core.c:2649 at _regulator_put+0x80/0xa0, CPU#6: kworker/u32:4/596 ... Call trace: _regulator_put+0x80/0xa0 (P) regulator_resolve_supply+0x7cc/0xbe0 regulator_register_resolve_supply+0x28/0xb8 as the regulator_list_mutex must be held when calling _regulator_put(). To solve this, simply switch to using regulator_put(). While at it, we should also make sure that no concurrent access happens to our rdev while we clear out the supply pointer. Add appropriate locking to ensure that. While the code in question will be removed altogether in a follow-up commit, I believe it is still beneficial to have this corrected before removal for future reference.	5.5	More Details
CVE-2025-71313	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: Add missing NULL check for alloc_workqueue() alloc_workqueue() can return NULL on memory allocation failure. Without proper error checking, this may lead to a NULL pointer dereference when queue_work() is later called with the NULL workqueue pointer in epf_ntb_epc_init(). Add a NULL check immediately after alloc_workqueue() and return -ENOMEM on failure to prevent the driver from loading with an invalid workqueue pointer.	5.5	More Details
CVE-2025-71314	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Recover from panthor_gpu_flush_caches() failures We have seen a few cases where the whole memory subsystem is blocked and flush operations never complete. When that happens, we want to: - schedule a reset, so we can recover from this situation - in the reset path, we need to reset the pending_reqs so we can send new commands after the reset - if more panthor_gpu_flush_caches() operations are queued after the timeout, we skip them and return -EIO directly to avoid needless waits (the memory block won't miraculously work again) Note that we drop the WARN_ON()s because these hangs can be triggered with buggy GPU jobs created by the UMD, and there's no way we can prevent it. We do keep the error messages though. v2: - New patch v3: - Collect R-b - Explicitly mention the fact we dropped the WARN_ON()s in the commit message v4: - No changes	5.5	More Details
CVE-2026-44119	Improper Privilege Management vulnerability in Apache HTTP Server 2.4.67 and earlier allows local .htaccess authors to read files with the privileges of the httpd user. This issue affects Apache HTTP Server: from through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	5.5	More Details
CVE-2026-46245	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix dc_link NULL handling in HPD init amdgpu_dm_hpd_init() may see connectors without a valid dc_link. The code already checks dc_link for the polling decision, but later unconditionally dereferences it when setting up HPD interrupts. Assign dc_link early and skip connectors where it is NULL. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_irq.c:940 amdgpu_dm_hpd_init() error: we previously assumed 'dc_link' could be null (see line 931) drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_irq.c 923 /* 924 * Analog connectors may be hot-plugged unlike other connector 925 * types that don't support HPD. Only poll analog connectors. 926 */ 927 use_polling |= 928 amdgpu_dm_connector->dc_link && ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ The patch adds this NULL check but hopefully it can be removed 929 dc_connector_supports_analog(amdgpu_dm_connector->dc_link->link_id.id); 930 931 dc_link = amdgpu_dm_connector->dc_link; dc_link assigned here. 932 933 /* 934 * Get a base driver irq reference for hpd ints for the lifetime 935 * of dm. Note that only hpd interrupt types are registered with 936 * base driver; hpd_rx types aren't. IOW, amdgpu_irq_get/put on 937 * hpd_rx isn't available. DM currently controls hpd_rx 938 * explicitly with dc_interrupt_set() 939 */ --> 940 if (dc_link->irq_source_hpd != DC_IRQ_SOURCE_INVALID) { ^^^^^^^^^^^^^^^^^^^^^^^^^^ If it's NULL then	5.5	More Details

	we are trouble because we dereference it here. 941 irq_type = dc_link->irq_source_hpd - DC_IRQ_SOURCE_HPD1; 942 /* 943 * TODO: There's a mismatch between mode_info.num_hpd 944 * and what bios reports as the # of connectors with hpd		
CVE-2026-50263	A use-after-free flaw was found in the X.Org X server and Xwayland in CreateSaverWindow(). A client can trigger a use-after-free read after changing window attributes and forcing the screen saver, leading to information disclosure.	5.5	More Details
CVE-2026-50262	An out-of-bounds read flaw was found in the X.Org X server and Xwayland in __glXDisp_ChangeDrawableAttributes(). A wrong size validation check can read a client-controlled number of bytes, exceeding the request buffer, leading to information disclosure. A write path also exists but requires byte-swapped clients which is disabled by default.	5.5	More Details
CVE-2026-46247	In the Linux kernel, the following vulnerability has been resolved: clk: qcom: gfx3d: add parent to parent request map After commit d228ece36345 ("clk: divider: remove round_rate() in favor of determine_rate()") determining GFX3D clock rate crashes, because the passed parent map doesn't provide the expected best_parent_hw clock (with the roundd_rate path before the offending commit the best_parent_hw was ignored). Set the field in parent_req in addition to setting it in the req, fixing the crash. clk_hw_round_rate (drivers/clk/clk.c:1764) (P) clk_divider_bestdiv (drivers/clk/clk-divider.c:336) divider_determine_rate (drivers/clk/clk-divider.c:358) clk_alpha_pll_postdiv_determine_rate (drivers/clk/qcom/clk-alpha-pll.c:1275) clk_core_determine_round_nolock (drivers/clk/clk.c:1606) clk_core_round_rate_nolock (drivers/clk/clk.c:1701) __clk_determine_rate (drivers/clk/clk.c:1741) clk_gfx3d_determine_rate (drivers/clk/qcom/clk-rcg2.c:1268) clk_core_determine_round_nolock (drivers/clk/clk.c:1606) clk_core_round_rate_nolock (drivers/clk/clk.c:1701) clk_core_round_rate_nolock (drivers/clk/clk.c:1710) clk_round_rate (drivers/clk/clk.c:1804) dev_pm_opp_set_rate (drivers/opp/core.c:1440 (discriminator 1)) msm_devfreq_target (drivers/gpu/drm/msm/msm_gpu_devfreq.c:51) devfreq_set_target (drivers/devfreq/devfreq.c:360) devfreq_update_target (drivers/devfreq/devfreq.c:426) devfreq_monitor (drivers/devfreq/devfreq.c:458) process_one_work (arch/arm64/include/asm/jump_label.h:36 include/trace/events/workqueue.h:110 kernel/workqueue.c:3284) worker_thread (kernel/workqueue.c:3356 (discriminator 2) kernel/workqueue.c:3443 (discriminator 2)) kthread (kernel/kthread.c:467) ret_from_fork (arch/arm64/kernel/entry.S:861)	5.5	More Details
CVE-2026-41980	Permission control vulnerability in the file preview module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2026-46248	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: clear stale link mapping of ahvif->links_map When an arvif is initialized in non-AP STA mode but MLO connection preparation fails before the arvif is created (arvif->is_created remains false), the error path attempts to delete all links. However, link deletion only executes when arvif->is_created is true. As a result, ahvif retains a stale entry of arvif that is initialized but not created. When a new arvif is initialized with the same link id, this stale mapping triggers the following WARN_ON. WARNING: drivers/net/wireless/ath/ath12k/mac.c:4271 at ath12k_mac_op_change_vif_links+0x140/0x180 [ath12k], CPU#3: wpa_supplicant/275 Call trace: ath12k_mac_op_change_vif_links+0x140/0x180 [ath12k] (P) drv_change_vif_links+0xbc/0x1a4 [mac80211] ieee80211_vif_update_links+0x54c/0x6a0 [mac80211] ieee80211_vif_set_links+0x40/0x70 [mac80211] ieee80211_prep_connection+0x84/0x450 [mac80211] ieee80211_mgd_auth+0x200/0x480 [mac80211] ieee80211_auth+0x14/0x20 [mac80211] cfg80211_mlme_auth+0x90/0xf0 [cfg80211] nl80211_authenticate+0x32c/0x380 [cfg80211] genl_family_rcv_msg_doit+0xc8/0x134 Fix this issue by unassigning the link vif and clearing ahvif->links_map if arvif is only initialized but not created. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.5-01651-QCAHKSWPL_SILICONZ-1	5.5	More Details
CVE-2026-21028	Improper access control in AuditLogService prior to SMR Jun-2026 Release 1 allows local attackers to access sensitive information.	5.5	More Details
CVE-2026-46249	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: Fix PF driver crash with kexec kernel booting During a kexec reboot the hardware is not power-cycled, so AF state from the old kernel can persist into the new kernel. When AF and PF drivers are built as modules, the PF driver may probe before AF reinitializes the hardware. The PF driver treats the RVUM block revision as an indication that AF initialization is complete. If this value is left uncleared at shutdown, PF may incorrectly assume AF is ready and access stale hardware state, leading to a crash. Clear the RVUM block revision during AF shutdown to avoid PF mis-detecting AF readiness after kexec.	5.5	More Details
CVE-2026-21026	Improper export of android application components in SpriteWallpaper prior to SMR Jun-2026 Release 1 allows local attackers to access to sensitive information.	5.5	More Details
CVE-	Incorrect privilege assignment in Telephony prior to SMR Jun-2026 Release 1 allows local attackers to		More

2026-21025	access sensitive information.	5.5	Details
CVE-2026-21017	Improper handling of insufficient privileges in SecTelephonyProvider prior to SMR Jun-2026 Release 1 allows local attackers to access privileged files.	5.5	More Details
CVE-2026-9751	The ldapQueryPassword parameter, when set through the runtime setParameter command, will log the new password to the mongod.log file in plain text.	5.5	More Details
CVE-2026-11516	A vulnerability was found in UTT HiPER 2610G up to 3.0.0-171107. This affects the function strcpy of the file /goform/formNatStaticMap. Performing a manipulation of the argument NatBinds results in buffer overflow. The exploit has been made public and could be used.	5.5	More Details
CVE-2026-34657	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in an arbitrary file system write. An attacker could leverage this vulnerability to write to unauthorized files or directories outside of intended restrictions. Exploitation of this issue requires user interaction in that a victim must extract a maliciously crafted file.	5.5	More Details
CVE-2026-11232	Inappropriate implementation in TabGroups in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	5.4	More Details
CVE-2026-41972	Path traversal vulnerability in the SMS app. Impact: Successful exploitation of this vulnerability may affect availability.	5.4	More Details
CVE-2026-26378	Cross Site Scripting vulnerability in Koha 25.11 and before allows a remote attacker to execute arbitrary code via file upload function in Invoice features	5.4	More Details
CVE-2026-36728	A markdown based cross-site scripting (XSS) vulnerability in the AI assistant chat function of FastapiAdmin v2.2.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into a chat message.	5.4	More Details
CVE-2026-11243	Inappropriate implementation in Downloads in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	5.4	More Details
CVE-2026-34033	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. User-supplied content was included in notification emails without proper escaping, allowing authenticated users to inject arbitrary HTML into emails sent to other users. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	5.4	More Details
CVE-2026-25557	Evoluted PHP Directory Listing Script through 4.0.5 contains a reflected cross-site scripting vulnerability in index.php where the dir parameter value is reflected without HTML encoding inside the HTML title element and inside anchor href attributes in the breadcrumb navigation. Attackers can inject arbitrary JavaScript via crafted dir parameter values by breaking out of the title context or injecting event handlers into breadcrumb anchor attributes to execute malicious scripts in a victim's browser.	5.4	More Details
CVE-2026-47106	Ellucian Banner Self-Service before the April T2 release (2025-04-23) contains a stored cross-site scripting vulnerability in the course search functionality that allows authenticated Banner ERP users to inject malicious payloads into faculty and course fields by exploiting missing HTML encoding during DOM insertion. Attackers can store malicious JavaScript in fields such as faculty displayName, emailAddress, subjectDescription, or courseTitle through the unauthenticated getFacultyMeetingTimes API endpoint, causing arbitrary script execution.	5.4	More Details
CVE-2026-34692	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-50591	In Znuny LTS before 6.5.21 and Znuny before 7.3.3, XSS can occur via stored user preferences.	5.4	More Details
CVE-2026-33113	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details

CVE-2026-47957	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-49192	The summary service endpoint suffers from an IDOR vulnerability where it fails to verify user ownership of hardware serial numbers, exposing device data to scraping.	5.4	More Details
CVE-2026-47958	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47983	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47982	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47981	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47980	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47978	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47977	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47975	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47974	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47935	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47973	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47972	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious		More

2026-47936	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	Details
CVE-2026-47939	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47941	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47942	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47943	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47944	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47945	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47970	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47966	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47947	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47948	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47949	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47950	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47951	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious	5.4	More

47953	scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.		Details
CVE-2026-47954	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47956	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47962	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47985	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47639	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-47986	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48268	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-45453	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-11157	Script injection in Accessibility in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to inject arbitrary scripts or HTML (UXSS) via a crafted Chrome Extension. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-48560	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-45464	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-45465	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-48304	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-48301	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-10984	Inappropriate implementation in Accessibility in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	5.4	More Details

CVE-2026-48300	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-48299	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-48297	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-48280	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48271	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-42547	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. In versions prior to 2.4.28, users can create alerts for customers that are not assigned to them. This can be abused to falsely attribute fake alerts to customers. In combination with Cross-Site Scripting, this can also be used to exfiltrate alerts from other customers. Version 2.4.28 contains a patch.	5.4	More Details
CVE-2026-47987	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48266	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-45595	Protection mechanism failure in Windows Mark of the Web (MOTW) allows an unauthorized attacker to bypass a security feature over a network.	5.4	More Details
CVE-2026-48265	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48264	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48258	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48256	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-40930	LIBPNG is a reference library for use in applications that process PNG (Portable Network Graphics) raster image files. In version 1.8.0, three inter-frame chunk discard paths in the push-mode APNG parser clear the chunk-header flag without consuming the chunk body and CRC, allowing attacker-controlled bytes inside an ignored ancillary chunk to be reinterpreted as a fresh chunk header on the next call to `png_process_data`. Commit faf06924688b62d7c1654b5ceddedbde66ffadb4 fixes the issue.	5.4	More Details
CVE-	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based		

2026-48251	Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-48250	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47993	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47990	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	5.4	More Details
CVE-2026-47989	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-47636	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-47946	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	5.4	More Details
CVE-2026-8833	Improper neutralization of HTML-encoded characters in the URL validation function in Checkmk <2.5.0p5, <2.4.0p31, <2.3.0p48, and all 2.2.0 versions allows an authenticated user to bypass URL validation and inject malicious URLs such as javascript: URIs, resulting in cross-site scripting when another user interacts with the crafted link.	5.4	More Details
CVE-2026-11466	A weakness has been identified in zilliztech deep-searcher up to 0.0.2. This affects the function CollectionRouter.invoke of the file deepsearcher/agent/collection_router.py. This manipulation of the argument kwargs causes improper access controls. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The pull request to fix this issue awaits acceptance.	5.4	More Details
CVE-2026-11701	Inappropriate implementation in Guest View in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-11533	A security vulnerability has been detected in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. Affected by this vulnerability is an unknown functionality of the file /see.php of the component Student Deletion Endpoint. The manipulation of the argument del leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-7186	Stored cross-site scripting in the URL dashboard widget in Checkmk <2.5.0p5, <2.4.0p31, <2.3.0p48, and all 2.2.0 versions allows a user with dashboard editing permissions to store a URL with a dangerous URI scheme such as javascript: that executes scripts in other users' browsers when they view the dashboard.	5.4	More Details
CVE-2026-11666	Insufficient validation of untrusted input in Input in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	5.4	More Details
CVE-2026-11569	A flaw was found in Quay. The filedrop endpoint accepts any mime type without validation, allowing an authenticated user with repository write access to upload a malicious SVG file containing JavaScript. The file is stored and served inline through the CDN, enabling stored cross-site scripting when a victim visits the archive URL.	5.4	More Details
	A security vulnerability has been detected in jishenghua jshERP up to 3.6. This vulnerability affects the		

CVE-2026-11467	function addAccountHeadAndDetail of the file jshERP-boot/src/main/java/com/jsh/erp/service/AccountHeadService.java of the component addAccountHeadAndDetail Endpoint. Such manipulation of the argument fileName leads to path traversal. The attack can be executed 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.	5.4	More Details
CVE-2026-7792	The WPForms – Easy Form Builder for WordPress – Contact Forms, Payment Forms, Surveys, & More plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in versions up to and including 1.10.0.1. This is due to the PayPal Commerce webhook endpoint processing unauthenticated JSON webhook payloads without verifying that the request originated from PayPal using the required HMAC-SHA256 webhook signature, and only checking whether the supplied event_type is whitelisted before dispatching the attacker-controlled resource data to handlers that update payment records. This makes it possible for unauthenticated attackers who know a valid PayPal subscription_id to forge PayPal webhook events and modify subscription payment records, such as reactivating a cancelled or suspended subscription by setting its subscription_status to active.	5.3	More Details
CVE-2026-42914	Windows Kerberos Denial of Service Vulnerability	5.3	More Details
CVE-2026-41178	OpenTelemetry-Go is the Go implementation of OpenTelemetry. Versions 1.41.0 and 1.43.0 removed raw-length rejection and it causes `Parse` to process arbitrarily large/invalid baggage headers and log errors, enabling DoS via oversized inputs. Versions 1.42.0 and 1.44.0 fix the issue.	5.3	More Details
CVE-2020-25900	HelloTalk through 3.4.1 stores full-precision GPS coordinates even when the user had intended to share only a country or city. Furthermore, these coordinates are placed into a database on the client of other users. (The client side was changed in 2019 to encrypt that database.)	5.3	More Details
CVE-2024-27891	On affected platforms running Arista EOS with MACsec and egress ACLs configured on the same interfaces, the ACL policies may not be enforced for packets egressing on those ports. This can cause outgoing packets to incorrectly be allowed or denied.	5.3	More Details
CVE-2026-11669	Out of bounds read in Media in Google Chrome on ChromeOS prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-50233	Lyrion Music Server 9.2.0 contains an arbitrary directory listing vulnerability in its readdirectory query, exposed through both the CLI service (TCP port 9090) and the HTTP JSON-RPC endpoint (/jsonrpc.js). The query accepts a folder parameter and lists its contents with no restriction to the configured media directories and no authentication in the default configuration, allowing a remote, unauthenticated attacker to enumerate arbitrary locations on the host filesystem.	5.3	More Details
CVE-2026-8608	The Event Monster – Event Management, Events Calendar, Tickets plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in versions up to, and including, 2.1.0. This is due to the capture_payment() AJAX handler (registered via wp_ajax_nopriv_em_capture_payment) trusting client-supplied payment data — including transaction ID, amount, and payment status — without performing any server-side verification against the PayPal API or any other payment gateway, and without nonce or capability checks. This makes it possible for unauthenticated attackers to forge payment records, mark bookings as Completed, and obtain confirmation emails containing valid QR code tickets without making any actual payment.	5.3	More Details
CVE-2026-50226	Fixed AES-128-CBC keys inside the AcerConnect OTA application let attackers forge authorization credentials for arbitrary IMEI numbers. This allows unauthorized actors to list catalog items and extract protected binaries from pre-signed cloud links.	5.3	More Details
CVE-2026-11174	Inappropriate implementation in Site Isolation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-11487	A flaw has been found in Neovim up to 0.12.2. Affected by this issue is the function M.read of the file runtime/lua/vim/secure.lua of the component View Branch. Executing a manipulation of the argument path can lead to command injection. It is possible to launch the attack on the local host. The exploit has been published and may be used. This patch is called f83e0dcaf8cf18de94828341b0a1a61a86c75baf. A patch should be applied to remediate this issue.	5.3	More Details
CVE-2026-10597	OMICARD EDM developed by ITPison has a Insecure Direct Object Reference vulnerability, allowing unauthenticated remote attackers to modify a specific parameter to obtain user's email address.	5.3	More Details
CVE-2026-	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory	5.3	More

11004	via a crafted HTML page. (Chromium security severity: Medium)		Details
CVE-2026-50589	In OpenStack Ironic 32 before 37.0.0, an unauthenticated malicious user could submit a crafted JSON string to some endpoints on the API or JSON-RPC service and effect a service crash.	5.3	More Details
CVE-2026-11515	A vulnerability has been found in SourceCodester Barangay Resident Profiling and Information Management System 1.0. The impacted element is an unknown function of the file passsword_reset.php of the component Password Reset Handler. Such manipulation of the argument new_password with the input password123 leads to use of hard-coded password. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2026-11005	Out of bounds read in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-41207	The netty incubator codec.bhttp is a java language binary http parser. Prior to version 0.0.21.Final, HKDF_expand returns non-NULL on failure. The byte[] is filled with zeros and has no way to distinguish success from failure. Since this output is used as HKDF key material for the response AEAD, a failure silently produces an all-zero key. When EVP_HPKE_CTX_export fails it also returns an empty byte[] array filled with zeros. This byte[] feeds directly into OHttpCrypto.createResponseAEAD(...). A silent all-zero export secret would produce a deterministic, attacker-predictable AEAD key. Version 0.0.21.Final patches the issue.	5.3	More Details
CVE-2026-44545	daphne before 4.2.2 did not pass maxFramePayloadSize or maxMessagePayloadSize to Autobahn's WebSocketServerFactory. Because Autobahn defaults both values to 0 (unlimited), an unauthenticated remote attacker could send arbitrarily large WebSocket messages or frames, causing excessive memory consumption and a denial of service.	5.3	More Details
CVE-2026-47706	Strawberry GraphQL is a library for creating GraphQL APIs. In versions 0.71.0 through 0.315.6, the QueryDepthLimiter extension is vulnerable to an Application-level DOS due to a lack of cycle detection in fragment spreads. When a query contains circular fragment references the determine_depth function enters an infinite recursion, leading to a RecursionError and crashing the validation process. Version 0.315.7 patches the issue.	5.3	More Details
CVE-2026-11620	A security flaw has been discovered in TOTOLINK EX200 4.0.3c.7646. This affects an unknown function of the file /etc/vsftpd.conf of the component vsftpd. The manipulation results in least privilege violation. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	5.3	More Details
CVE-2026-26825	A use-of-uninitialized memory vulnerability exists in libxls 1.6.3 when parsing malformed XLS files. The issue is reachable via xls_parseWorkBook() and is triggered by uninitialized heap memory originating from the OLE layer (ole2_read). The flaw is detectable with MemorySanitizer (MSAN) and can lead to undefined behavior, incorrect parsing logic, or potential information disclosure.	5.3	More Details
CVE-2026-11145	Race in Geolocation in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-11497	A vulnerability has been found in D-Link DCS-5615 1.01.00. Affected by this vulnerability is an unknown functionality of the file /etc/conf.d/boa/boa.conf of the component Boa Webserver. Such manipulation leads to least privilege violation. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2026-11098	Insufficient validation of untrusted input in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2026-47707	Strawberry GraphQL is a library for creating GraphQL APIs. In versions 0.172.0 through0.315.6, the MaxAliasesLimiter extension in Strawberry fails to account for the multiplicative/amplification effect of FragmentSpreadNode. While it correctly counts static aliases within the AST it does not consider how many times a fragments internal aliases are expanded during execution. this allows an attacker to bypass alias limits and force the server to resolve and render a significantly higher number of aliases than allowed, potentially leading to a dos via resource exhaustion. Version 0.315.7 contains a fix for the issue.	5.3	More Details
	Issue Summary: An error in the callback used to verify the certificate provided in a Root CA key update Certificate Management Protocol (CMP) message response rendered the certificate validation ineffectual, which could lead to escalation of credentials from the Registration Authority (RA) level to the root Certification Authority (root CA) level. Impact Summary: The Registration Autority could replace the root CA certificate for the CMP clients with an arbitrary root CA certificate. One of the parts of the Certificate		

CVE-2026-42769	Management Protocol (CMP), specified in RFC 9810, is Root Certification Authority (root CA) key Rollover, which is sent by the server in a message with type 'id-it-rootCaKeyUpdate'. As part of these messages, 'newWithOld' certificate, the new root CA certificate signed with the old root CA key, is provided, and verifying its signature is crucial for transferring the trust from the old CA key to the new one. The 'id-it-rootCaKeyUpdate' messages are expected to be processed with OSSL_CMP_get1_rootCaKeyUpdate(), that is expected to verify the 'newWithOld' certificate. A typo in the certificate chain building code led to adding an incorrect certificate ('newWithOld' instead of 'oldRoot') to the certificate chain, rendering the certificate verification process ineffectual (only the issuer name and the algorithm OIDs were verified by other parts of the verification code). An attacker who already has credentials that satisfy the CMP message protection checks can generate a new key pair and use a crafted self-signed certificate in its 'id-it-rootCaKeyUpdate' CMP messages which affected CMP clients would accept as a new trust anchor. Significant preconditions for the attack (having valid RA-level credentials) are the reason the issue was assigned Low severity. The FIPS modules are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	5.3	More Details
CVE-2026-49955	Hermes WebUI before version 0.51.270 contains a resource exhaustion vulnerability that allows unauthenticated remote attackers to degrade service availability by repeatedly calling the passkey options endpoint without completing assertion. Attackers can send unlimited POST requests to the authentication endpoint, causing unbounded growth of the challenge store file and excessive CPU and disk I/O through repeated JSON file rewrites.	5.3	More Details
CVE-2026-11678	Integer overflow in libyuv in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details
CVE-2026-46739	Net::Statsd versions before 0.13 for Perl allow metric injections. The metric names are not checked for newlines, colons or pipes. Metrics generated from untrusted sources could inject additional statsd metrics. The update_stats (used for updating counters) and gauge methods do not check that values are numeric (which would block metric injection).	5.3	More Details
CVE-2026-7665	The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 6.6.4 via the ajax_load_more function due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft posts that they should not have access to.	5.3	More Details
CVE-2026-11246	Insufficient validation of untrusted input in IndexedDB in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	5.3	More Details
CVE-2026-8499	The Helpfulcrowd Product Reviews plugin for WordPress is vulnerable to Authorization Bypass via PHP Type Juggling in versions up to, and including, 1.2.9. This is due to the `helpfulcrowd_validate_token()` function using a loose comparison operator (`!=`) instead of a strict comparison (`!==`) when validating the `token` parameter, while the corresponding REST route `/wp-json/helpfulcrowd/v1/update-settings` is registered with a `permission_callback` of `__return_true`, making it reachable by unauthenticated users; submitting a JSON boolean `true` as the `token` value causes PHP's loose comparison to evaluate as equal to the non-empty base64-encoded secret string, bypassing the check entirely. This makes it possible for unauthenticated attackers to invoke `helpfulcrowd_settings_endpoint()` and write arbitrary attacker-controlled key-value pairs directly into the `helpfulcrowd_options` WordPress database option via `update_option()` without any sanitization or allowlist filtering, enabling full unauthenticated modification of the plugin's stored configuration.	5.3	More Details
CVE-2026-8839	The MapPress Maps for WordPress plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to, and including, 2.96.6. This is due to missing ownership verification in the REST API routes registered via `Mappress_Api::rest_api_init()`, where the GET `/wp-json/mapp/v1/maps/{mapid}` endpoint uses `'permission_callback' => '__return_true'` and the write endpoints (POST update, DELETE, PATCH mutate, POST clone, POST empty_trash) only check the generic `edit_posts` capability without confirming that the requester owns the targeted map — a gap that is not compensated at the model layer, as `Mappress_Map::get()`, `save()`, `delete()`, `mutate()`, and `empty_trash()` all operate on any caller-supplied map ID without an ownership check. This makes it possible for unauthenticated attackers to read sensitive map data — including POI titles, addresses, coordinates, and body content — for any map on the site by enumerating map IDs, and for authenticated attackers with Contributor-level access and above to modify, delete, trash/restore, or clone any map regardless of its author.	5.3	More Details
CVE-2026-11696	Uninitialized Use in Video in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	5.3	More Details

CVE-2026-4986	The WPForms WordPress plugin before 1.10.0.5 does not verify the authenticity of incoming PayPal webhook events before processing them, allowing unauthenticated attackers to forge webhook payloads and manipulate the payment state of arbitrary transactions.	5.3	More Details
CVE-2026-11552	A vulnerability has been found in SourceCodester Onlne Examination & Learning Management System and Syllabus-aligned Learning Management and Examination System 1.0. Affected by this issue is some unknown functionality of the file import_users.php. The manipulation of the argument raw_password with the input CICT_2026 leads to use of hard-coded password. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This product is distributed under two entirely different names.	5.3	More Details
CVE-2026-11458	A weakness has been identified in erzhongxmu JeeWMS up to 141740afb2ba14d441c82a833d0a418d07ca2d69. This issue affects some unknown processing of the file /base-boot/actuator of the component Boot Actuator Endpoint. Executing a manipulation can lead to information disclosure. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-9016	The Debug Log Manager – Conveniently Monitor and Inspect Errors plugin for WordPress is vulnerable to Improper Output Neutralization for Logs in all versions up to, and including, 2.5.0. This is due to the `log_js_errors()` AJAX handler being registered for unauthenticated users via `wp_ajax_nopriv_log_js_errors` and gated only by a nonce that is publicly disclosed in every front-end page's HTML through `wp_localize_script()` whenever JavaScript error logging is enabled, providing no real authorization barrier. This makes it possible for unauthenticated attackers to inject arbitrary forged entries into the site's WordPress debug log by supplying attacker-controlled values for the `message`, `script`, `lineNo`, `columnNo`, and `pageUrl` fields — enabling spoofing of error and incident records, obscuring malicious activity within fabricated log noise, and misleading administrators who rely on the log for triage. This vulnerability is only exploitable when the plugin's JavaScript error logging feature is enabled, as the requisite nonce is only published into the page HTML under that condition.	5.3	More Details
CVE-2026-40898	quic-go is an implementation of the QUIC protocol in Go. Prior to version 0.59.1, an attacker can cause excessive memory allocation in quic-go's HTTP/3 client and server implementations by sending a QPACK-encoded HEADERS frame that decodes into a large trailer field section with many unique field names and/or large values. The implementation builds an `http.Header` for the corresponding `http.Request` or `http.Response`, while only enforcing limits on the size of the QPACK-compressed HEADERS frame, not on the decoded field section. This can lead to memory exhaustion. This is very similar to CVE-2025-64702. The difference is that this issue uses HTTP trailers, rather than HTTP headers, as the attack vector. A misbehaving or malicious peer can cause a denial-of-service (DoS) attack against quic-go's HTTP/3 servers or clients by triggering excessive memory allocation, potentially leading to crashes or resource exhaustion. This affects both servers and clients due to symmetric header construction. Version 0.59.1 enforces RFC 9114 decoded field section size limits for trailers as well. It incrementally decodes QPACK entries and checks the field section size after each entry, aborting the stream if an entry causes the limit to be exceeded.	5.3	More Details
CVE-2026-49843	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, mod_verto's JSON-RPC handler bound the connection to the client-supplied sessid on the first frame, before the authentication gate. Binding inserts the connection into the global session hash and, on a key collision, drops the prior occupant of that slot — sending it a verto.punt, detaching its calls, and closing its socket. An unauthenticated network attacker who knows a target session UUID could therefore evict the legitimate client. This issue has been patched in version 1.11.1.	5.3	More Details
CVE-2026-41851	Applications which accept user-supplied Spring Expression Language (SpEL) expressions may be vulnerable to a Denial of Service (DoS) attack if the evaluation of a SpEL expression triggers unbounded cache growth. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	5.3	More Details
CVE-2026-41981	Out-of-bounds write vulnerability in the IPC module. Impact: Successful exploitation of this vulnerability may affect availability.	5.3	More Details
CVE-2026-7765	Incorrect authorization in the User Messages dashboard widget in Checkmk <2.5.0p5 causes the message-fetching endpoints to return the dashboard creator's messages rather than the viewer's, allowing an attacker who knows a valid public dashboard share token to read the issuer's personal messages by sending requests to the underlying endpoint, even without a User Messages widget present.	5.3	More Details
CVE-2026-	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	5.3	More Details

45655			
CVE-2026-49472	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.0, FreeSWITCH includes a vulnerable function, PREFIX(prologTok)(), in libs/xmlrpc-c/lib/expat/xmltok/xmltok_impl.c, which was cloned from an outdated and vulnerable version in libexpat/libexpat. The function did not receive the corresponding security patch. This issue has been patched in version 1.11.0.	5.3	More Details
CVE-2026-5078	Impact: The morgan logging middleware's :remote-user token extracts the Basic auth username from the Authorization request header and writes it to the log stream without neutralizing control characters. An unauthenticated attacker can send a crafted Authorization Basic header containing CR or LF bytes to inject forged log lines, breaking the one-request-per-line structure of access logs and enabling log forgery against downstream log consumers. The built-in combined, common, default, and short formats are affected, as well as any custom format that references :remote-user. Affected versions: morgan 1.2.0 through 1.10.1. Patches: upgrade to morgan 1.11.0, which neutralizes control characters in the :remote-user token output. Workarounds: use a custom format string that does not include :remote-user.	5.3	More Details
CVE-2026-8502	The LearnPress – WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.6 via the 'return_type' parameter. This makes it possible for unauthenticated attackers to extract sensitive data including the plaintext post_password of password-protected courses and the full post_content, post_author, and post_name of unpublished draft, private, and pending courses via the unrestricted SELECT * fallback query. Exploitation requires supplying both c_status=all (to bypass the publish-only post_status WHERE clause) and return_type=json (to prevent the safe DISTINCT(ID) AS ID field override) in a single unauthenticated request to the /wp-json/lp/v1/courses/archive-course endpoint.	5.3	More Details
CVE-2026-49077	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Tips and Tricks HQ WP eMember allows Retrieve Embedded Sensitive Data. This issue affects WP eMember: from n/a through v10.2.2.	5.3	More Details
CVE-2026-41853	Spring MVC and WebFlux applications are vulnerable to Multipart request smuggling attacks. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	5.3	More Details
CVE-2026-41984	UAF vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	5.2	More Details
CVE-2026-41985	UAF vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	5.1	More Details
CVE-2026-11276	Inappropriate implementation in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to bypass discretionary access control via malicious network traffic. (Chromium security severity: Low)	5.1	More Details
CVE-2026-11787	A flaw was found in 389 Directory Server. The ldap_utf8prev() function reads bytes before the start of a buffer without bounds checking, causing a heap buffer over-read in string filter parsing that may influence internal filter processing behavior.	5.0	More Details
CVE-2026-11455	A vulnerability was determined in FoundationAgents MetaGPT up to 0.8.2. Affected by this issue is the function check_cmd_exists of the file metagpt/utils/common.py. This manipulation of the argument mermaid.path causes command injection. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitation is known to be difficult. 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.	5.0	More Details
CVE-2026-11493	A weakness has been identified in Tenda AC15 15.03.05.19. The impacted element is an unknown function of the file /etc_ro/smb.conf of the component Samba. Executing a manipulation can lead to weak password requirements. The attack is only possible within the local network. A high complexity level is associated with this attack. The exploitability is regarded as difficult. The exploit has been made available to the public and could be used for attacks.	5.0	More Details
CVE-2026-49958	Hermes WebUI before version 0.51.303 contains a time-of-check time-of-use (TOCTOU) race condition vulnerability in the git_discard function within api/workspace_git.py that allows attackers to delete files outside the configured workspace boundary by replacing a validated path component with a symlink after validation but before deletion. Attackers can substitute a workspace-controlled path component with a symlink pointing to an external directory between the safe_resolve_ws() validation step and the subsequent Path.unlink() or shutil.rmtree() deletion call, causing the delete operation to follow the	5.0	More Details

	symlink and remove arbitrary files outside the workspace.		
CVE-2026-11500	A vulnerability was identified in Weaviate up to 1.37.7. This vulnerability affects the function validateConfig of the file usecases/auth/authentication/apikey/client.go of the component Static API Key Handler. The manipulation of the argument StaticApiKey leads to authorization bypass. It is possible to initiate the attack remotely. The complexity of an attack is rather high. It is stated that the exploitability is difficult. The exploit is publicly available and might be used. Upgrading to version 1.38.0-rc.0 is able to resolve this issue. The identifier of the patch is 40f2cc32279f0f8a51016c3c6870a2c0c808e6c0. You should upgrade the affected component.	5.0	More Details
CVE-2026-11281	Integer overflow in Chromoting in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted ETW event. (Chromium security severity: Low)	5.0	More Details
CVE-2026-45502	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to disclose information over a network.	5.0	More Details
CVE-2025-60477	A NULL pointer dereference in the gf_filter_pid_resolve_file_template_ex function (/filter_core/filter_pid.c) of GPAC Project/MP4Box before 26.02.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted file.	5.0	More Details
CVE-2026-11505	A flaw has been found in GL.iNet A1300, AX1800, AXT1800, MT2500, MT3000, MT6000, X3000 and XE3000 4.8.x. This affects an unknown function of the component glnassys. Executing a manipulation can lead to use of hard-coded cryptographic key . The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is reported as difficult. Upgrading to version 4.9.0 mitigates this issue. Upgrading the affected component is advised.	5.0	More Details
CVE-2026-41977	DoS vulnerability in the log service. Impact: Successful exploitation of this vulnerability may affect availability.	5.0	More Details
CVE-2026-11290	Integer overflow in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to cause a denial of service via a malicious file. (Chromium security severity: Low)	5.0	More Details
CVE-2026-6448	The Quiz and Survey Master (QSM) – Easy Quiz and Survey Maker plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'order' parameter in all versions up to, and including, 11.1.2 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 admin-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. If the secret key is exposed, this can be exploited by lower-privileged users.	4.9	More Details
CVE-2026-50219	libexpat before 2.8.2 lacks handler call depth tracking for calls to XML_GetBuffer, XML_Parse, XML_ParseBuffer, XML_ParserFree, or XML_ParserReset from within handlers in cases of a policy violation. Thus, a use-after-free can occur,	4.9	More Details
CVE-2026-11789	A flaw was found in 389 Directory Server. The SMD5 password storage plugin performs unsigned integer underflow when computing salt length from a crafted password hash shorter than 16 bytes, causing a buffer over-read that crashes the LDAP server during authentication.	4.9	More Details
CVE-2026-11790	A flaw was found in 389 Directory Server. The PBKDF2-SHA256 password storage plugin does not enforce an upper bound on the iteration count extracted from stored password hashes. A privileged attacker who can modify a user's password hash can cause excessive CPU consumption during authentication, resulting in denial of service.	4.9	More Details
CVE-2026-11793	A stack buffer overflow flaw was found in 389 Directory Server. The checkPrefix() function in pw.c copies an attacker-controlled algorithm ID into a 256-byte stack buffer without bounds checking when parsing reversible-encrypted attribute values. An attacker with Directory Manager privileges can crash the LDAP server by storing a crafted credential with an oversized algorithm ID. FORTIFY_SOURCE mitigates this to denial of service only.	4.9	More Details
CVE-2026-50224	The web administration panel binds broadly to the public IPv6 address space on port [::]:8080 without default firewall limits, making internal API endpoints reachable over the WAN.	4.9	More Details
CVE-2026-9197	The Smart Slider 3 plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.5.1.36 via the replaceHTMLImage function. This makes it possible for authenticated attackers, with administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details

CVE-2026-7565	The LearnPress – Backup & Migration Tool plugin for WordPress is vulnerable to Arbitrary File Read via Directory Traversal in all versions up to, and including, 4.1.4 via the 'import-user-file' parameter parameter. This makes it possible for authenticated attackers, with administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2026-8978	The OptinCraft – Drag & Drop Optins & Popup Builder for WordPress plugin for WordPress is vulnerable to generic SQL Injection via the 'order_by' parameter in all versions up to, and including, 1.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-44917	OpenStack Ironic before 35.0.2 allows a malicious authenticated project admin or manager to read local files on the Ironic conductor via a pxe_template.	4.9	More Details
CVE-2026-41838	IDs for WebSocket sessions in the spring-websocket module are not cryptographically unpredictable, which may be possible to exploit in combination with inadequate authorization rules. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	4.8	More Details
CVE-2026-41847	Spring WebFlux applications may be vulnerable to a security bypass when using the Kotlin Router DSL. Affected versions: Spring Framework 5.3.0 through 5.3.48.	4.8	More Details
CVE-2026-8078	Stored cross-site scripting in the global settings change log in Checkmk <2.5.0p5, <2.4.0p31, <2.3.0p48, and all 2.2.0 versions allows an administrator who can change global settings to store malicious HTML or JavaScript in changelog messages that executes in other users' browsers when they view the Activate Changes page or Audit log.	4.8	More Details
CVE-2026-25558	QloApps through 1.7.0 contains a stored cross-site scripting vulnerability in the admin file manager that allows authenticated administrators to inject malicious JavaScript by uploading crafted SVG files. Attackers can embed JavaScript event handlers such as onload within SVG files uploaded through the file manager to execute arbitrary scripts in the browser of any user who subsequently views the file.	4.8	More Details
CVE-2026-45446	Issue summary: The implementations of AES-SIV (RFC 5297) and AES-GCM-SIV (RFC 8452) mishandle the authentication of AAD (Additional Authenticated Data) with an empty ciphertext allowing a forgery of such messages. Impact summary: An attacker can forge empty messages with arbitrary AAD to the victim's application using these ciphers. AES-SIV (RFC 5297) and AES-GCM-SIV (RFC 8452) are nonce-misuse-resistant AEAD modes: they accept a key, nonce, optional AAD (bytes that are authenticated but not encrypted), and plaintext, and produces ciphertext plus a 16-byte tag. On decrypt, `EVP_DecryptFinal_ex()` is documented to return success only if the tag is verified succesfully. In OpenSSL's provider implementation of these ciphers, the expected tag is computed only when decryption function is invoked with non-empty data. If the caller supplies AAD and then calls `EVP_DecryptFinal_ex()` without invocation of the ciphertext update, which can happen when the received ciphertext length is zero, the tag is never recalculated and still holds its all-zeros value. When AES-GCM-SIV is used, an attacker who sends arbitrary AAD, empty ciphertext, and all-zeros tag passes authentication under any key they do not know, single-shot. When AES-SIV is used, for mounting the attack it's necessary for the application to reuse the decryption context without resetting the key. AES-SIV is implemented since OpenSSL 3.0. AES-GCM-SIV is implemented since OpenSSL 3.2. No protocols implemented in OpenSSL itself (TLS/CMS/PKCS7/HPKE/QUIC) support either AES-GCM-SIV or AES-SIV. To mount an attack, the applications must implement their own protocol and use the EVP interface. Also they must skip the ciphertext update when a message with an empty ciphertext arrives. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as these algorithms are not FIPS approved and the affected code is outside the OpenSSL FIPS module boundary.	4.8	More Details
CVE-2026-36460	Dovestones Softwares ADPhonebook before v4.0.1.1 is vulnerable to a Cross Site Scripting vulnerability. The /Admin/Save API allows an authenticated admin user to store malicious JavaScript payloads in multiple configuration sections without proper input validation or output encoding.	4.8	More Details
CVE-2026-47933	ColdFusion versions 2023.19, 2025.8 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	4.8	More Details
CVE-2026-9549	Stored cross-site scripting in the service discovery active check output in Checkmk <2.5.0p5, <2.4.0p31, <2.3.0p48, and all 2.2.0 versions allows an administrator who can configure active or custom checks to inject malicious HTML or JavaScript into check output that executes in the browser of an admin or a user with host read permissions when they run the check on the service discovery page.	4.8	More Details

CVE-2026-28301	A vulnerability in which an attacker can provide a crafted external URL that may redirect a user to an unintended website.	4.8	More Details
CVE-2026-44757	SAP Wily Introscope Enterprise Manager allows an unauthenticated attacker to craft a specially crafted URL. Under certain conditions, when accessed by a victim, the injected script could execute in the user's browser within the context of the application. This issue has a low impact on the confidentiality and integrity of the application with no impact on availability.	4.7	More Details
CVE-2026-46272	In the Linux kernel, the following vulnerability has been resolved: coresight: tmc-etr: Fix race condition between sysfs and perf mode When trying to run perf and sysfs mode simultaneously, the WARN_ON() in tmc_etr_enable_hw() is triggered sometimes: WARNING: CPU: 42 PID: 3911571 at drivers/hwtracing/coresight/coresight-tmc-etr.c:1060 tmc_etr_enable_hw+0xc0/0xd8 [coresight_tmc] [..snip..] Call trace: tmc_etr_enable_hw+0xc0/0xd8 [coresight_tmc] (P) tmc_enable_etr_sink+0x11c/0x250 [coresight_tmc] (L) tmc_enable_etr_sink+0x11c/0x250 [coresight_tmc] coresight_enable_path+0x1c8/0x218 [coresight] coresight_enable_sysfs+0xa4/0x228 [coresight] enable_source_store+0x58/0xa8 [coresight] dev_attr_store+0x20/0x40 sysfs_kf_write+0x4c/0x68 kernfs_fop_write_iter+0x120/0x1b8 vfs_write+0x2c8/0x388 ksys_write+0x74/0x108 __arm64_sys_write+0x24/0x38 el0_svc_common.constprop.0+0x64/0x148 do_el0_svc+0x24/0x38 el0_svc+0x3c/0x130 el0t_64_sync_handler+0xc8/0xd0 el0t_64_sync+0x1ac/0x1b0 ---[end trace 0000000000000000]--- Since the enablement of sysfs mode is separeted into two critical regions, one for sysfs buffer allocation and another for hardware enablement, it's possible to race with the perf mode. Fix this by double check whether the perf mode's been used before enabling the hardware in sysfs mode. mode: [sysfs mode] [perf mode] tmc_etr_get_sysfs_buffer() spin_lock(&drvdata->spinlock) [sysfs buffer allocation] spin_unlock(&drvdata->spinlock) spin_lock(&drvdata->spinlock) tmc_etr_enable_hw() drvdata->etr_buf = etr_perf->etr_buf spin_unlock(&drvdata->spinlock) spin_lock(&drvdata->spinlock) tmc_etr_enable_hw() WARN_ON(drvdata->etr_buf) // WARN sicne etr_buf initialized at the perf side spin_unlock(&drvdata->spinlock) With this fix, we retain the check for CS_MODE_PERF in get_etr_sysfs_buf. This ensures we verify whether the perf mode's already running before we actually allocate the buffer. Then we can save the time of allocating/freeing the sysfs buffer if race with the perf mode.	4.7	More Details
CVE-2026-42329	Iris is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 contain a weakness where an attacker can misuse it to redirect the user to a malicious website controlled by an attacker. Version 2.4.28 fixes the issue.	4.7	More Details
CVE-2026-45614	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Prior to version 4.11.0, on many of the ECDH shared secret paths, the public key isn't verified to be a point on the correct curve. By passing approximately 30-40 crafted public keys to OP-TEE, the private key can be reconstructed by a normal world attacker. When calling TEE_DeriveKey the public key is provided with full X and Y values, but the (X, Y) point might not satisfy the `Y^2 == X^3 + aX + b mod P` math for the specific curve that is used. When those public keys aren't rejected, the attacker can select public keys such that each DeriveKey call will leak `d % r` where `d` is the private key and `r` comes from the relationship between the correct curve and the attacker selected curve. With enough leaked data the Chinese remainder theorem can be used to recover the full private key. Version 4.11.0 fixes the issue.	4.7	More Details
CVE-2026-11448	A weakness has been identified in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function realpath of the file /rpc of the component Minidlna Service. This manipulation of the argument kube. set causes command injection. The attack is possible to be carried out remotely. Upgrading to version 4.7 is sufficient to fix this issue. It is recommended to upgrade the affected component. The vendor confirms: "Starting from version 4.7, SDK has added global protection to intercept malicious injection".	4.7	More Details
CVE-2026-11233	Insufficient policy enforcement in FoldableAPIs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	4.7	More Details
CVE-2026-11621	A weakness has been identified in Dcat-Admin up to 2.2.3-beta. This impacts the function editorMDUpload of the file /admin/dcat-api/editor-md/upload of the component User Setting Page. This manipulation of the argument editormd-image-file causes unrestricted upload. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	4.7	More Details
CVE-2026-52902	A path traversal vulnerability was found in awxkit, the CLI tool for AWX. The YAML !include directive does not sanitize file paths, allowing an attacker to craft a malicious YAML file that reads arbitrary YAML-formatted files from the local filesystem when a user imports it using "awx --conf.format yaml import". This is a client-side vulnerability requiring user interaction.	4.7	More Details
CVE-	A flaw has been found in jishenghua jshERP up to 3.6. Impacted is the function insertPlatformConfig of the file jshERP-boot/src/main/java/com/jsh/erp/service/PlatformConfigService.java of the component		

2026-11469	platformConfig Add Endpoint. Executing a manipulation of the argument platformValue can lead to server-side request forgery. The attack may be performed from remote. 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.	4.7	More Details
CVE-2026-45460	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	4.7	More Details
CVE-2026-11249	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	4.7	More Details
CVE-2026-45467	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-47638	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-47640	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-36174	GNCC GP5 v7.1.76 was discovered to store sensitive wireless network information in plaintext during routine operations to the serial console. This issue allows physically-proximate attackers to obtain sensitive information, including network credentials, via monitoring the serial UART interface.	4.6	More Details
CVE-2026-48562	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-36178	The factory reset functionality in GNCC GP5 v7.1.76 fails to clear sensitive cryptographic material in the JFFS2 configuration partition, possibly allowing attackers to recover and obtain sensitive user data.	4.6	More Details
CVE-2026-36180	A lack of runtime integrity in GNCC GP5 v7.1.76 allows physically-proximate attackers to bypass file system read-only protections and modify system files and binaries for the duration of a boot session via a bind-mount attack.	4.6	More Details
CVE-2026-47641	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-45468	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-45462	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-45483	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office Project Server allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-47637	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-45479	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-50590	In Mimecast Incydr before 2.6.0, arbitrary file access can occur.	4.5	More Details
	A security vulnerability has been detected in tmux up to 3.6a. Affected is the function image_free of the file image.c. Such manipulation leads to use after free. Local access is required to approach this attack.		

CVE-2026-11623	This attack is characterized by high complexity. The exploitability is told to be difficult. The exploit has been disclosed publicly and may be used. Upgrading to version 3.7-rc is able to address this issue. The name of the patch is fc6d94a9f8a593bd8b7031650802084385d4ee03. The affected component should be upgraded.	4.5	More Details
CVE-2026-10814	A vulnerability has been found in milvus-io milvus up to 2.6.13. This vulnerability affects unknown code of the file internal/metastore/kv/rootcoord/kv_catalog.go of the component Grantee ID Hash Handler. The manipulation leads to use of weak hash. The attack needs to be performed locally. The attack's complexity is rated as high. It is stated that the exploitability is difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is 3d932f1c3e065351c4440c27abe1e6479752544d. Applying a patch is the recommended action to fix this issue.	4.5	More Details
CVE-2026-9594	The WP Maps – Google Maps,OpenStreetMap,Mapbox,Store Locator,Listing,Directory & Filters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'location_messages' parameter in all versions up to, and including, 4.9.4 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. Exploitation requires the attacker to hold the custom wpgmp_manage_location capability, which is granted to administrators by default but can be assigned to lower-privileged roles via the plugin's Permissions screen.	4.4	More Details
CVE-2026-11411	A security flaw has been discovered in iAI Lab PDF AI App 4.21.0 on Android. Impacted is the function getExternalCacheDir of the component chatpdf.pro. Performing a manipulation of the argument _display_name results in path traversal. The attack requires a local approach. 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.	4.4	More Details
CVE-2026-7421	The Passeum Ticketing plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.0. This is due to the `get_shop_url()` method returning the `shop_name` setting value without sanitization when it begins with "http", combined with insufficient validation in the `validate_shop_name()` function which only checks for empty values and string type. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary external scripts by setting the `shop_name` to an attacker-controlled URL (e.g., `https://attacker.com`), which causes the plugin to enqueue external JavaScript and CSS from the attacker-controlled domain via `wp_register_script()` and `wp_register_style()`. The injected scripts execute on every frontend page containing any Passeum Ticketing shortcode, affecting all site visitors. Please note that this does not affect single-site installations as administrators already have the `unfiltered_html` capability.	4.4	More Details
CVE-2026-45702	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 4.3.0 and prior to version 4.11.0, a type confusion vulnerability exists in OP-TEE OS when processing an FFA_MEM_SHARE request from the normal world. This only applies when OP-TEE is configured as an SPMC for S-EL0 SPs, that is, with `CFG_CORE_SEL1_SPMC=y` and `CFG_SECURE_PARTITION=y`. Version 4.11.0 fixes the issue.	4.4	More Details
CVE-2026-8991	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'drag_n_drop_text' and 'drag_n_drop_browse_text' Settings in all versions up to, and including, 1.3.9.7 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.	4.4	More Details
CVE-2026-41978	Permission control vulnerability in the clone module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.4	More Details
CVE-2026-2500	The Quick Playground plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.4. This is due to the `qckply_data()` function passing the user-supplied `filename` POST parameter directly to `file_get_contents()` without any validation, sanitization, or path restriction. This makes it possible for authenticated attackers, with Administrator-level access and above, to read arbitrary files on the server, such as `wp-config.php` or `/etc/passwd`, which can contain sensitive information. Note: This vulnerability is only exploitable when the site has been synced with WordPress Playground (the `is_qckply_clone` option is set) or when running on `playground.wordpress.net`.	4.4	More Details
CVE-2026-11261	Inappropriate implementation in PDF in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11254	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE-2026-11257	Inappropriate implementation in Browser in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-44755	SAP Business Objects Business Intelligence Platform does not sufficiently validate email sending parameters supplied by authenticated users, resulting in an email spoofing vulnerability.This vulnerability has a low impact on integrity and does not affect the confidentiality and availability of the application.	4.3	More Details
CVE-2026-11264	Policy bypass in Content Security Policy in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-44750	SAP MDG (Review Match Groups Application) does not perform the necessary authorization checks for authenticated users. This could allow a low-privileged user to perform actions that would otherwise be restricted, resulting in escalation of privileges. This has a low impact on integrity, while confidentiality and availability are not impacted.	4.3	More Details
CVE-2026-11267	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11266	Inappropriate implementation in SafeBrowsing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass Safe Browsing via a malicious file. (Chromium security severity: Low)	4.3	More Details
CVE-2026-10855	An authorization flaw existed in the MISP Event Template Importer overwrite workflow. When importing an event template in overwrite mode, the application checked whether a matching template already existed but did not verify that the importing user belonged to the organization that owned the existing template. As a result, an authenticated user with access to the template import functionality could forcibly overwrite an event template owned by another organization. Successful exploitation could allow unauthorized modification of another organization’s event template, potentially altering template structure, attributes, or metadata used for subsequent event creation or sharing workflows. Site administrators are not affected by this restriction, as they are explicitly allowed to overwrite templates across organizations. The issue was fixed by enforcing an ownership check before overwrite: non-site-admin users may only overwrite templates owned by their own organization.	4.3	More Details
CVE-2026-11259	Insufficient validation of untrusted input in Cast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11274	Inappropriate implementation in DOM Distiller in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11260	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-48103	7-Zip is a file archiver with a high compression ratio. Versions 9.34 through 26.00 contain an off-by-one heap out-of-bounds read in the WIM (Windows Imaging) archive handler's security descriptor lookup. In CHandler::GetSecurity (CPP/7zip/Archive/Wim/WimHandler.cpp), the per-image SecurOffsets table holds numEntries + 1 cumulative offsets, but the check securityId >= SecurOffsets.Size() admits securityId == numEntries, and the function then reads SecurOffsets[securityId + 1], fetching one UInt32 past the end of the heap-allocated CRecordVector (which performs no bounds checking on operator[]). The securityId is attacker-controlled at offset +0xC of any directory entry in WIM metadata, and the handler is registered for .wim, .swm, .esd, and .ppkg and enabled by default in stock 7z.dll; the OOB triggers zero-click in the GUI because 7zFM.exe's ListView calls GetRawProp(kpidNtSecure) for every item during listing (ASan-confirmed), and is also reachable via CLI listing with 7zz l -slt. Impact is limited to denial of service under hardened allocators and minor information disclosure, since the OOB value is only consumed arithmetically as a length and is not surfaced to the attacker; there is no write primitive.	4.3	More Details
CVE-2026-11253	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-	The Charitable – Donation Plugin for WordPress – Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to Insecure Direct Object Reference / Authorization Bypass leading to Arbitrary Attachment Deletion in versions up to, and including, 1.8.11.1 via the profile avatar update flow. This is due to the save_avatar() function in Charitable_Profile_Form calling wp_delete_attachment() on an attachment ID read from the user's 'avatar' meta without validating that the attachment is owned by the		More

2026-10038	user, combined with Charitable_Data_Processor::process_picture() returning the raw posted value when no file is uploaded, allowing the 'avatar' user meta to be poisoned with any attacker-chosen attachment ID. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary attachments from the Media Library by performing a two-request chain (first poisoning the stored avatar meta value with a target attachment ID, then triggering deletion via a normal avatar upload).	4.3	Details
CVE-2026-11155	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-45650	User interface (ui) misrepresentation of critical information in Microsoft Bing allows an unauthorized attacker to perform spoofing over a network.	4.3	More Details
CVE-2026-11126	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11107	Inappropriate implementation in Downloads in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11062	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11031	Insufficient validation of untrusted input in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-7624	The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 12.4.16. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to invoke privileged state-changing Squirrly cloud API operations, such as revoking the site's Google Search Console and Google Analytics integrations via `api/gsc/revoke` and `api/ga/revoke`, that are otherwise restricted to administrator-level users holding the `sq_manage_settings` capability.	4.3	More Details
CVE-2026-7047	The Frontend User Notes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.1. This is due to missing or incorrect nonce validation on the funp_ajax_modify_notes function. This makes it possible for unauthenticated attackers to trick a logged-in user into visiting a malicious page, causing unauthorized overwriting of that victim's own note content via a forged cross-site request to wp_update_post() via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Due to ownership enforcement comparing the note's stored _funp_single_user_id meta against the current session's user ID, the attack is limited to modifying only notes belonging to the tricked victim, and cannot be used to alter notes owned by arbitrary third-party users.	4.3	More Details
CVE-2026-11668	Uninitialized Use in Codecs in Google Chrome on Linux, ChromeOS prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted video file. (Chromium security severity: High)	4.3	More Details
CVE-2026-8976	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.1.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to create and execute RSS import jobs, purge (force-delete) all posts associated with any import job, clear import error logs, and enumerate taxonomy terms and post meta_key names. The nonce required to reach these sub-handlers is leaked to any user with the edit_posts capability via the feedzyjs localized script injected into the block editor, meaning no privileged nonce theft or separate exploit step is required for Contributor-level users.	4.3	More Details
CVE-2026-42543	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 are vulnerable to a cross-site request forgery attack, because they use the HTTP method `GET` to change state on the server. Version 2.4.28 contains a patch.	4.3	More Details
CVE-2026-42540	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 allow a user to alter values in the database via manipulated API requests. Version 2.4.28 contains a patch.	4.3	More Details
CVE-2026-	Out of bounds read in Dawn in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote	4.3	More

11665	attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)		Details
CVE-2026-9719	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, 5.6.0. This is due to missing or incorrect nonce validation on the change_status function. This makes it possible for unauthenticated attackers to change the status of arbitrary invoices — including marking unpaid invoices as paid — without administrator consent 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-2026-9008	The Page-list plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 6.2. This is due to the pagelist_unqprfx_ext_shortcode() function (the [pagelist_ext] / [pagelistext] shortcode) accepting attacker-controlled post_status, post_type, and show_meta_key attributes and passing them directly into get_pages() and get_post_meta() with no capability check verifying that the rendering user is permitted to read the matched objects. When the current post has no child pages, the shortcode re-issues the query with child_of => 0, broadening it to every page on the site matching the supplied status/type. This makes it possible for authenticated attackers, with contributor-level access and above, to disclose the titles, body content/excerpts, and arbitrary post meta of unrelated private and draft pages by inserting the shortcode into a contributor-authored draft and previewing it.	4.3	More Details
CVE-2026-11156	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11277	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11252	Insufficient policy enforcement in Content Settings in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11161	Inappropriate implementation in DataTransfer in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11245	Inappropriate implementation in Payments in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-8611	The Klamra Paycal for Aspaclaria plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.4 via the 'invoice_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to download arbitrary customer invoices by enumerating sequential post IDs, exposing sensitive billing PII including full name, email address, phone number, order total, line items, and customer notes belonging to other customers.	4.3	More Details
CVE-2026-11695	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-11234	Inappropriate implementation in FoldableAPIs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-10864	A vulnerability in the MISP dashboard widgets allowed an authenticated user to manipulate the fields option and influence which fields were returned by the New Users and New Organisations widgets. In some cases, requesting a field set that became empty after validation or redaction could cause the underlying query to fall back to returning unintended model fields. For the New Users widget, this could allow a non-site-admin user to obtain user e-mail addresses even when user e-mail disclosure was disabled by configuration. For the New Organisations widget, crafted field selection could similarly result in unintended organisation fields being included in the dashboard response. The issue was caused by applying field filtering and redaction in a way that could leave the selected field list empty. The patch ensures that the allowed field list is built safely, that restricted fields such as user e-mail addresses are removed before user-supplied field selection is processed, and that an empty field selection falls back only to the permitted default fields. Impact: An authenticated low-privileged user with access to the affected dashboard widgets may be able to disclose restricted user or organisation metadata, including user e-mail addresses depending on configuration.	4.3	More Details
CVE-2026-	Inappropriate implementation in File Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted	4.3	More Details

11228	HTML page. (Chromium security severity: Low)		
CVE-2026-11221	Insufficient validation of untrusted input in PointerLock in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11219	Inappropriate implementation in Navigation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11216	Incorrect security UI in File Input in Google Chrome prior to 149.0.7827.53 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)	4.3	More Details
CVE-2026-11212	Insufficient policy enforcement in DevTools in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11192	Insufficient validation of untrusted input in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11685	Inappropriate implementation in MediaCapture in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-7523	The Alba Board plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.1.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to access arbitrary private alba_card post data, including title, description, assignee, due date, tags, and comments, that is intended to be restricted to Administrators and Editors. The handler is registered via the wp_ajax_nopriv_ hook and its nonce is exposed to all site visitors through wp_localize_script on pages containing the [alba_board] shortcode, making this exploitable by unauthenticated users who can access any such page.	4.3	More Details
CVE-2026-11178	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11162	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-11159	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-10810	A weakness has been identified in itsourcecode Fees Management System up to 1.0. Affected is an unknown function of the file /navbar.php. This manipulation of the argument page causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-11280	Inappropriate implementation in Signin in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-36613	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 returns 128 bytes of uninitialized internal buffer contents when receiving HTTP POST requests to undefined paths, exposing server state to unauthenticated adjacent network attackers.	4.3	More Details
CVE-2026-47991	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Redirect (Open Redirect) vulnerability that could lead to account takeover. An attacker could construct a malicious URL that redirects a victim to an attacker-controlled site. Exploitation of this issue requires user interaction in that a victim must click on a malicious link.	4.3	More Details
CVE-2026-10802	A vulnerability was detected in keystonejs keystone up to 20260319. This vulnerability affects unknown code in the library packages/core/src/lib/core/queries/output-field.ts of the component GraphQL API Endpoint. The manipulation results in resource consumption. It is possible to launch the attack remotely. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.	4.3	More Details
CVE-	HCL iControl was affected by Weak Input Validation vulnerability. This weakness is caused during		

2025-52606	implementation of an architectural security tactic. Received input that is expected to be of a certain type, but it does not validate or incorrectly validates that the input is actually of the expected type.	4.3	More Details
CVE-2026-49848	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, mod_verto's check_auth userauth branch wrote request-supplied userVariables into the connection state before comparing the supplied password. The writes are append-only and the connection is not closed on a failed compare, so values declared on bad-password attempts persisted on the same WebSocket and carried into a subsequent successful login on that connection. This issue has been patched in version 1.11.1.	4.3	More Details
CVE-2026-8909	The WpMobi plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.0.3. This is due to missing or incorrect nonce validation on the handleSaveGeneralSettings function. This makes it possible for unauthenticated attackers to modify the plugin's General Settings and inject arbitrary web scripts into the administrator's browser via the unescaped app_name attribute reflection via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The injected script executes even when the supplied app_name value fails validation and is not persisted to the database, because the form is re-rendered with the attacker-supplied in-memory value on validation failure.	4.3	More Details
CVE-2026-11785	A flaw was found in 389 Directory Server. A type confusion in the SSO token extended operation handler causes partial stack address information to be disclosed in LDAP responses to authenticated users.	4.3	More Details
CVE-2026-11285	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11492	A security flaw has been discovered in D-Link DIR-823G 1.0.2B05. The affected element is an unknown function of the file /etc/vsftpd.conf of the component vsftpd. Performing a manipulation results in least privilege violation. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	4.3	More Details
CVE-2026-11494	A security vulnerability has been detected in TOTOLINK AC1200 T8 4.1.5cu.8611. This affects an unknown function of the file /etc/vsftpd.conf of the component vsftpd. The manipulation leads to least privilege violation. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-36618	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 responds to version.bind CHAOS TXT queries, disclosing the DNS resolver software version (unbound 1.22.0), aiding targeted attacks against known vulnerabilities.	4.3	More Details
CVE-2026-36615	Mercusys AC12G (EU) V1 with firmware AC12G(EU)_V1_200909 exposes an undocumented /agileconfigreset endpoint that returns internal buffer contents to unauthenticated attackers on the adjacent network.	4.3	More Details
CVE-2026-36602	Mercusys AC12G (EU) V1 router with firmware AC12G(EU)_V1_200909 discloses kernel memory layout via the UPnP GetStatusInfo action. An unauthenticated attacker on the adjacent network can obtain a raw MIPS KSEG0 kernel pointer, revealing kernel memory layout and aiding further exploitation.	4.3	More Details
CVE-2026-11554	A vulnerability was determined in TOTOLINK CP450 4.1.0cu.747. This vulnerability affects unknown code of the file /etc/vsftpd.conf of the component vsftpd. This manipulation causes least privilege violation. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-11512	A security vulnerability has been detected in itsourcecode Hospital Management System 1.0. This issue affects some unknown processing of the file /billing.php. The manipulation of the argument patientid leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-4058	The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the user_subscription_cancel() function in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to cancel any user's subscription pack, including administrators.	4.3	More Details
CVE-2026-46747	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected application does not properly sanitize path input in the `GET /api/sftp/uploadFiles` endpoint used for directory listing. This allows path traversal through crafted input, enabling access to unintended file system locations.	4.3	More Details
CVE-2024-	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Backup Task functionality in Synology Hyper Backup before 4.1.2-4036 allows remote authenticated users to	4.3	More

47273	write specific files via unspecified vectors.		Details
CVE-2026-48092	7-Zip is a file archiver with a high compression ratio. Versions 9.34 through 26.00 contain a heap memory disclosure via SquashFS fragment offset integer overflow on 32-bit builds. 32-bit integer overflow in the SquashFS ReadBlock function allows an attacker-controlled node.Offset value to bypass the fragment bounds check, causing memcpy to read heap memory preceding the cache buffer into the extracted file. The vulnerability is exploitable only on 32-bit builds of 7-Zip where size_t is 32 bits, allowing the addition offsetInBlock + blockSize to wrap modulo 2^{32}. On 64-bit builds the addition is promoted to 64 bits and the check correctly rejects the input. Version 26.01 patches the issue.	4.3	More Details
CVE-2026-41983	DoS vulnerability in the browser kernel. Impact: Successful exploitation of this vulnerability may affect availability.	4.3	More Details
CVE-2026-11518	A vulnerability was identified in SourceCodester Inventory System 1.0. Affected is an unknown function of the file /users.php of the component User Management Page. The manipulation of the argument fullname/username leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-9732	The EmergencyWP – Dead Man's switch & legacy deliverance plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.2. This is due to missing or incorrect nonce validation on the form_settings_ui (settings save handler, procedural include scope) function. This makes it possible for unauthenticated attackers to modify plugin settings including the minimum access role (altering WordPress role capabilities via add_cap/remove_cap), the data-erasure-on-uninstall flag, life-check timing values, the mandator email address, the confirmation page ID, and date/time formats 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-2026-10692	A weakness has been identified in johnhuang316 code-index-mcp up to 2.14.0. Affected is the function is_safe_regex_pattern of the component search_code_advanced. Executing a manipulation of the argument regex can lead to inefficient regular expression complexity. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.14.1 is able to address this issue. This patch is called 25bc02fac74051ddae15ce79e952f00211b1ea6b. Upgrading the affected component is recommended.	4.3	More Details
CVE-2026-11337	A vulnerability was found in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. Affected by this vulnerability is an unknown functionality of the file /dashboard_page/forms/fetch.php. The manipulation of the argument department_name results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-8940	The WP Meta Sort Posts plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.9. This is due to missing or incorrect nonce validation on the top-level included script in msp-options.php. This makes it possible for unauthenticated attackers to change the plugin's msp_loop_file and msp_nav_location settings via a forged request 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-2026-11477	A vulnerability was detected in hs-web hsweb-framework up to 5.0.1. This affects the function OAuth2Client of the file hsweb-authorization/hsweb-authorization-oauth2/src/main/java/org/hswebframework/web/oauth2/server/OAuth2Client.java of the component OAuth2 Client. The manipulation results in open redirect. The attack can be executed remotely. The exploit is now public and may be used. The patch is identified as c2882679a9125cea52678151af5ae213cbd52579. Applying a patch is advised to resolve this issue.	4.3	More Details
CVE-2026-8904	The FastPicker, an order picker and order management system (oms) for WooCommerce on steroids plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing or incorrect nonce validation on the settingsPage function. This makes it possible for unauthenticated attackers to modify the plugin's settings, including toggling the webhook integration and changing the FastPicker and KDZ API URLs 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
	7-Zip is a file archiver with a high compression ratio. Versions 9.21 through 26.00 contain an off-by-one out-of-bounds read vulnerability in the ParseDepedencyExpression function of the UEFI firmware image parser(CPP/7zip/Archive/UefiHandler.cpp). The function validates an attacker-controlled opcode byte using > instead of >= against the element count of the 10-entry kExpressionCommands static array, allowing an opcode value of 10 to read one pointer slot (8 bytes on x64) past the end of the array in		

CVE-2026-48111	.rodata. The out-of-bounds value is then dereferenced as a const char * and passed through strlen and memcpy into the archive's Charcts property, which may cause either a denial of service (access violation when the adjacent bytes do not form a valid readable pointer) or a minor information disclosure of an adjacent .rdata string literal into archive metadata. The vulnerability is reached automatically during IInArchive::Open() via the call path OpenFv/OpenCapsule → ParseVolume → ParseSections when processing a SECTION_DXE_DEPEX (0x13) or SECTION_PEI_DEPEX (0x1B) section whose first body byte is 0x0A, and the UEFI handler is enabled by default in stock 7z.dll with signature-based detection for both UEFIc and UEFIf formats. The outcome (crash vs. silent leak) is deterministic per build but linker-layout dependent, with no write primitive and no disclosure of heap data, secrets, or ASLR base addresses. Version 26.01 fixes the issue.	4.3	More Details
CVE-2026-8902	The AJAX Report Comments plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.4. This is due to missing or incorrect nonce validation on the rc_options_page function. This makes it possible for unauthenticated attackers to modify plugin settings including link text and markup, success/failure/already-reported messages, comment threshold, cookie duration, reporter-comment toggle, and notification email address, subject, and message body 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-2026-11286	Insufficient validation of untrusted input in Wallet in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-10787	Missing authorization in the deleted user groups API in Devolutions Server allows an authenticated low-privileged user to enumerate metadata of deleted user groups via a crafted API request. This issue affects : * Devolutions Server 2026.2.4.0 * Devolutions Server 2026.1.20.0 and earlier	4.3	More Details
CVE-2026-11291	Inappropriate implementation in Android Autofill in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11292	Insufficient policy enforcement in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11294	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11298	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11436	A vulnerability was detected in Mage AI up to 0.9.79. This impacts the function useMutation of the file mage_ai/frontend/components/Sessions/SignForm/index.tsx of the component Sign-in Flow. Performing a manipulation of the argument query.redirect_url results in cross site scripting. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-10553	The jQuery Hover Footnotes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or incorrect nonce validation on the jqFootnotes_options_subpanel function. This makes it possible for unauthenticated attackers to update the plugin's settings with arbitrary values that, because option values such as jqfoot_anchor_open, jqfoot_anchor_close, and jqfoot_title are echoed unescaped into frontend page content, can be chained into persistent Cross-Site Scripting affecting all site visitors via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Successful exploitation of the CSRF vulnerability can be chained into stored Cross-Site Scripting, as the overwritten option values are persisted via update_option() without sanitization and rendered unescaped on the frontend.	4.3	More Details
CVE-2026-11300	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-10691	A security flaw has been discovered in wonderwhy-er DesktopCommanderMCP up to 0.2.38. This impacts an unknown function of the file src/search-manager.ts of the component start_search. Performing a manipulation of the argument SearchResult[] results in inefficient regular expression complexity. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.2.39 will fix this issue. The patch is named 4ce845f8749b6a159b57b38dcc3357f7222a8078. It is suggested to upgrade the affected component.	4.3	More Details

CVE-2026-11302	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-11309	Insufficient policy enforcement in History in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-10854	A visibility control issue in the event template creation workflow allowed non-site-admin users to access private galaxies belonging to other organisations. The event template builder loaded all enabled galaxies without applying organisation or distribution-based access restrictions, potentially exposing private galaxy metadata such as galaxy type and description to users who should not have visibility. The issue has been fixed by restricting galaxy queries for non-site-admin users to galaxies owned by the user's organisation or galaxies with a non-private distribution setting. Site administrators retain visibility of all enabled galaxies.	4.3	More Details
CVE-2026-41844	A Spring MVC or Spring WebFlux application which configures a mapping for "/**" where the view name is not explicitly specified allows an attacker to craft a link resulting in a 302 redirect to an arbitrary external host via the redirect: prefix. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	4.2	More Details
CVE-2026-41839	A WebFlux application with a compromised subdomain (for example, compromised via cross-site scripting (XSS)) is vulnerable to an escalation attack exchanging a known session ID for that of an authenticated user. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	4.2	More Details
CVE-2026-41854	Due to incorrect host parsing, applications that rely on UriComponentsBuilder to parse and validate an externally provided URL string may be exposed to a server-side request forgery (SSRF) attack. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18.	4.2	More Details
CVE-2026-48104	7-Zip is a file archiver with a high compression ratio. Versions 9.18 through 26.00 contain an uninitialized heap read in the SquashFS archive handler caused by a sparsely populated index array. In the SquashFS handler, _blockToNode is allocated with capacity for every metadata block but populated only when an inode crosses a block boundary, so a crafted image with few inodes spanning many blocks leaves most slots holding raw heap contents (the underlying allocator does not zero-initialize POD storage). When OpenDir looks up an attacker-influenced blockIndex (derived from the RootInode superblock field), it reads two of these uninitialized slots and passes them as the left/right bounds of a binary search over _nodesPos, which dereferences the midpoint without bounds checking; if the resulting value happens to match the search key, the returned index is used to read a full node struct from _nodes whose fields feed further directory parsing, forming a chained OOB read primitive that is heap-layout-dependent and not reliably triggerable. The SquashFS handler is enabled by default in stock 7z.dll and the issue triggers during Open() with no interaction beyond opening the file; impact is denial of service from wild-pointer dereference and potential heap information disclosure, with no write primitive. Version 26.01 fixes the issue.	4.2	More Details
CVE-2026-24315	SAP Fiori Launchpad allows attackers to craft malicious URLs that triggers arbitrary service calls on the Fiori domain, this when opened by the user could compromise accounts by stealing user credentials. Successful exploitation requires adversaries to possess advanced knowledge of the system causing low impact on Confidentiality and Integrity. Availability of the system is no impacted.	4.2	More Details
CVE-2026-11479	A vulnerability has been found in yoanbernabeu grepai 0.35.0. This issue affects some unknown processing of the file indexer/chunker.go of the component Qdrant Backend. Such manipulation leads to use of weak hash. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	4.2	More Details
CVE-2026-37700	Cross Site Scripting vulnerability in MaxSite CMS v.109.2 allows a remote attacker to obtain sensitive information via the Backend page file upload endpoint used by admin_page	4.1	More Details
CVE-2024-47263	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Backup.Repository webapi component in Synology Hyper Backup before 4.1.2-4036 allows remote authenticated users with administrator privileges to write specific files containing non-sensitive information via unspecified vectors.	4.1	More Details
CVE-2026-10998	Out of bounds read in Media in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to perform an out of bounds memory read via malicious network traffic. (Chromium security severity: Medium)	4.0	More Details
	Contact Form by WD 1.13.1 contains a cross-site request forgery vulnerability combined with local file		

CVE-2019-25734	inclusion that allows unauthenticated attackers to include arbitrary files by exploiting unsanitized action parameters. Attackers can craft malicious forms targeting the admin-ajax.php endpoint with directory traversal sequences in the GET action parameter to load files via CSRF, bypassing authentication on vulnerable AJAX actions.	4.0	More Details
CVE-2026-45642	Improper input validation in Microsoft Azure Attestation service and Device Health Attestation Service allows an authorized attacker to perform spoofing with a physical attack.	3.9	More Details
CVE-2025-12656	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary directory deletion due to insufficient file path validation in the delete_cancel_staging_site() function in all versions up to, and including, 0.9.128. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary folders on the server, which leads to a loss of data.	3.8	More Details
CVE-2026-44743	Under certain conditions, when an unauthorized attacker accesses a specific endpoint, SAP Business Objects application leaks sensitive information .This has a low impact on the confidentiality of the data. There is no impact on integrity and availability of the application.	3.7	More Details
CVE-2026-42770	Issue summary: When EVP_PKEY_derive_set_peer() is called with a DHX (X9.42) peer key, the peer key is not properly checked for the subgroup membership. Impact summary: A malicious peer which presents an X9.42 key carrying the victim's p and g parameters, a forged q = r (a small prime factor of the cofactor (p−1)/q_local), and a public value Y of order r can recover the victim's private key after a small number of key exchange attempts. When EVP_PKEY_derive_set_peer() is called with a DHX (X9.42) peer key, the subgroup membership check Y^q ≡ 1 (mod p) is performed using the peer's own q parameter, not the local key's q. The peer's domain parameters are then matched against the domain parameters of the private key, but the value of q is not compared. A malicious peer who presents an X9.42 key carrying the victim's p, g, a forged q = r (a small prime factor of the cofactor), and a public value Y of order r passes all checks. The shared secret then takes only r distinct values, leaking priv mod r. Repeating for each small-prime factor of the cofactor and combining via CRT recovers the full private key (Lim–Lee / small-subgroup-confinement attack). The realistic attack surface is narrow: principally CMP deployments with long-lived RA/CA DHX keys and bespoke enterprise or government applications using X9.42 DHX static keys with interactive protocols and therefore this issue was assigned Low severity. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are affected by this issue.	3.7	More Details
CVE-2026-41852	A vulnerability in Spring Expression Language (SpEL) evaluation logic allows for arbitrary zero-argument method invocation, even within restricted or read-only contexts, which may allow an attacker to invoke unintended application logic. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	3.7	More Details
CVE-2025-52609	HCL iControl was affected by Missing Security Headers vulnerability. which lead to cross-site scripting (XSS) attacks by enabling the built-in XSS filtering mechanisms of modern web browsers.	3.7	More Details
CVE-2026-41848	Applications may be vulnerable to a Regular Expression Denial of Service (ReDoS) attack if an attacker is able to provide a pattern which is then directly or indirectly supplied to one of the following methods in AntPathMatcher: match(String pattern, String path), matchStart(String pattern, String path), extractUriTemplateVariables(String pattern, String path). Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	3.7	More Details
CVE-2026-44546	daphne before 4.2.2 reconstructs a raw HTTP request from Twisted's parsed headers and feeds it to autobahn for WebSocket handshake processing. Twisted does not treat \x0b, \x0c, \x1c, \x1d, \x1e, or \x85 as header line separators, but autobahn decodes header values to str and calls splitlines(). An attacker can exploit this parser differential to inject additional headers into the ASGI scope passed to the application. daphne now rejects requests with these bytes in any header value with a 400 response.	3.7	More Details
CVE-2026-11555	A vulnerability was identified in D-Link DGS-1100-08PD 1.00.006. This issue affects some unknown processing of the file /etc/boa.conf of the component Web Interface. Such manipulation leads to least privilege violation. The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is assessed as difficult. The exploit is publicly available and might be used.	3.7	More Details
	Issue summary: The CMS_decrypt and PKCS7_decrypt functions are vulnerable to Bleichenbacher-style attack when an attacker is able to provide the CMS or S/MIME messages and observe the error code and/or decryption output. Impact summary: The Bleichenbacher-style attack allows an attacker to use the victim's vulnerable application as a way to decrypt or sign messages with the victim's private RSA key. The attack is possible in 2 variants. 1. The decryption API (CMS_decrypt(), PKCS7_decrypt()) is used without providing the recipient certificate. In this case OpenSSL iterates over every KeyTransRecipientInfo (KTRI) without stopping at the first success. An attacker who authors a message with two KTRI entries — the first one wrapping a real CEK under the victim's public key, the second with an arbitrary probe ciphertext — obtains opportunity to iterate the 2nd KTRI to get a valid PKCS#1 v1.5 padding if the error		

CVE-2026-42768	code of the application is available. That is a Bleichenbacher oracle (Bleichenbacher, CRYPTO '98): an adaptive-chosen-ciphertext side channel from which the attacker decrypts any RSA ciphertext to the victim's key or forges any PKCS#1 v1.5 signature under it. 2. When the decryption API (CMS_decrypt(), PKCS7_decrypt()) is provided with the recipient certificate, and the recipient is not found, a random key is substituted. An attacker who authors a message and is able to compare both error code and the result of the decryption, can mount a Bleichenbacher oracle. We are not aware of any applications that provide a remote attacker an opportunity to mount an attack described in these scenarios. We consider the existence of such application very unlikely, and for this reason this CVE has been evaluated as Low severity. To avoid these attacks, when RSA PKCS#1 v1.5 Key Transport is in use, the invoked EVP_PKEY_decrypt() will use the implicit rejection mechanism described in draft-irtf-cfrg-rsa-guidance. In previous OpenSSL releases the implicit rejection was explicitly disabled. The implicit rejection mechanism always returns a plaintext value, the symmetric key. This result is deterministic for the ciphertext and the private key. The length of the decryption result can happen to match the length of the key of the symmetric cipher that was used for the content encryption. When a certificate is not provided, the last RecipientInfo producing a key that looks valid will be used. It may cause getting garbage content on decryption. As a proper way to deal with this a recipient certificate has to be provided to identify the particular RecipientInfo for decryption. The FIPS modules in 4.0, 3.6, 3.5, and 3.4 are not affected by this issue, as CMS and S/MIME processing happens outside the OpenSSL FIPS module boundary.	3.7	More Details
CVE-2026-10766	A vulnerability has been found in mlrun up to 1.12.0-rc3. This impacts the function mlrun.utils.helpers.calculate_dataframe_hash of the file mlrun/utils/helpers.py of the component DataFrame Hash Handler. The manipulation leads to use of weak hash. The attack can only be performed from a local environment. The complexity of an attack is rather high. The exploitability is said to be difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	3.6	More Details
CVE-2026-10813	A flaw has been found in LMCache up to 0.4.6. This affects the function hex_hash_to_int16 of the file lmcache/integration/vllm/utils.py of the component KV Cache Handler. Executing a manipulation can lead to use of weak hash. The attack needs to be launched locally. The attack requires a high level of complexity. It is indicated that the exploitability is difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	3.6	More Details
CVE-2026-41974	Permission control vulnerability in service notifications. Impact: Successful exploitation of this vulnerability may affect availability.	3.6	More Details
CVE-2026-10803	A flaw has been found in MLflow up to 3.10.0. This issue affects the function mlflow.data.digest_utils of the file mlflow/data/digest_utils.py of the component Dataset Digest Computation. This manipulation causes use of weak hash. It is possible to launch the attack on the local host. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	3.6	More Details
CVE-2026-11330	A weakness has been identified in thedotmack claude-mem up to 11.0.1. The affected element is the function computeObservationContentHash of the file src/services/sqlite/observations/store.ts of the component Observation Content Hash Handler. This manipulation causes use of weak hash. The attack can only be executed locally. The attack's complexity is rated as high. The exploitability is described as difficult. Upgrading to version 12.0.0 is sufficient to fix this issue. Patch name: f32fda8b35e9fe9329f87da65c31149362a03f97. It is suggested to upgrade the affected component.	3.6	More Details
CVE-2026-10775	A vulnerability was determined in sgl-project SGLang up to 0.5.11. Affected by this vulnerability is the function data_hash of the component Cache Handler. This manipulation causes denial of service. The attack is restricted to local execution. A high degree of complexity is needed for the attack. The exploitation appears to be difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	3.6	More Details
CVE-2026-10800	A weakness has been identified in PaddlePaddle FastDeploy up to 2.4.1. Affected by this issue is the function hash_features of the file fastdeploy/multimodal/hasher.py of the component MultimodalHasher. Executing a manipulation can lead to use of weak hash. The attack requires local access. A high complexity level is associated with this attack. The exploitation is known to be difficult. This patch is called 374945747652a8d32965591c0c01a00c88b7067f. Applying a patch is advised to resolve this issue.	3.6	More Details
CVE-2026-10812	A vulnerability was detected in zilliztech GPTCache up to 0.1.44. Affected by this issue is the function BufferedReader.peek of the file gptcache/processor/pre.py of the component Cache Key Handler. Performing a manipulation of the argument input_data["image"] results in use of weak hash. The attack must be initiated from a local position. The attack is considered to have high complexity. The exploitation is known to be difficult. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.	3.6	More Details
CVE-	A security vulnerability has been detected in modelscope ms-swift up to 4.2.0. This affects the function Template._save_pil_image of the file swift/template/base.py of the component PIL Image Cache Key		

2026-10801	Handler. The manipulation leads to use of weak hash. An attack has to be approached locally. A high degree of complexity is needed for the attack. It is indicated that the exploitability is difficult. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	3.6	More Details
CVE-2026-11329	A vulnerability has been found in onnx onnx-mlir up to 0.5.0.0. Affected by this issue is the function generate_hash_key of the file src/Runtime/python/torch_onnxmlir/src/torch_onnxmlir/backend.py of the component Placeholder Node Cache Handler. Such manipulation leads to use of weak hash. An attack has to be approached locally. A high complexity level is associated with this attack. The exploitation is known to be difficult. The name of the patch is 72c5187ff6d13c2c2b3d3789b8f5faf99f08a5b4. Applying a patch is advised to resolve this issue.	3.6	More Details
CVE-2026-10804	A vulnerability has been found in Streamlit up to 1.53.0. Impacted is an unknown function in the library lib/streamlit/runtime/caching/hashing.py of the component Palette Handler. Such manipulation leads to use of weak hash. Local access is required to approach this attack. The attack requires a high level of complexity. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	3.6	More Details
CVE-2026-48289	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	3.5	More Details
CVE-2026-48288	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	3.5	More Details
CVE-2026-11520	A weakness has been identified in SourceCodester Inventory System 1.0. Affected by this issue is some unknown functionality of the file header.php. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Multiple parameters might be affected.	3.5	More Details
CVE-2026-11511	A weakness has been identified in Bolt CMS up to 3.7.5. This vulnerability affects unknown code of the file src/Storage/Field/Type/TextType.php of the component HTML Attribute Handler. Executing a manipulation of the argument style can lead to HTML 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 GitHub repository was archived by the owner and is now read-only. This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2026-8981	The Custom Block Builder WordPress plugin before 4.3.0 does not consistently check the unfiltered_html capability across all paths that write to its block template code fields, allowing administrators on multisite installations (or single-site installs with DISALLOW_UNFILTERED_HTML defined) to inject arbitrary JavaScript that executes for any visitor of pages embedding the affected block.	3.5	More Details
CVE-2026-11534	A vulnerability was detected in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. Affected by this issue is some unknown functionality of the file /add.php. The manipulation of the argument name/address/fname results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-11312	A vulnerability was found in bytedance InfiniStore up to 0.2.33. The impacted element is the function purge_kv_map in the library /src/infinistore.h of the component KV Map Handler. Performing a manipulation results in inefficient algorithmic complexity. The attack requires a local approach. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-11478	A flaw has been found in kokke tiny-regex-c up to f2632c6d9ed25272987471cdb8b70395c2460bdb. This vulnerability affects the function matchstar of the file re.c of the component Pattern Handler. This manipulation causes inefficient regular expression complexity. The attack is restricted to local execution. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-	HCL BigFix Cloud Lifecycle Management is affected by lack of input validation. This low-level flaw allows		More

2025-62338	unauthorized access and may lead to information exposure.	3.3	Details
CVE-2026-10722	A vulnerability has been found in cilium ebpf up to 0.21.0. This affects the function loadRawSpec of the file btf/btf.go of the component LoadCollectionSpec/LoadCollectionSpecFromReader. Such manipulation of the argument offset leads to integer overflow. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used. The name of the patch is 533dfc82fd228bfadf42ea7180c39de7d9af47fa. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-11792	A heap buffer overflow flaw was found in 389 Directory Server. When audit logging is enabled, the create_masked_entry_string() function in auditlog.c copies a fixed-length password mask into a precisely-sized heap buffer without checking available space. If a short cleartext password is logged (requiring non-default CLEAR password storage or a compromised replication peer), the copy overflows the buffer, corrupting heap memory and audit log output.	3.3	More Details
CVE-2026-45455	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	3.3	More Details
CVE-2026-11459	A security vulnerability has been detected in SecureAge CatchPulse up to 10.9.3. Impacted is an unknown function in the library saappctl.sys of the component IOCTL Handler. The manipulation leads to information disclosure. Local access is required to approach this attack. 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.	3.3	More Details
CVE-2026-45485	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	3.3	More Details
CVE-2026-45459	Protection mechanism failure in Microsoft Office Excel allows an unauthorized attacker to bypass a security feature locally.	3.3	More Details
CVE-2026-45466	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	3.3	More Details
CVE-2026-21027	Improper export of android application components in ImsSettings prior to SMR Jun-2026 Release 1 allows local attackers to trigger logging function.	3.3	More Details
CVE-2026-48102	7-Zip is a file archiver with a high compression ratio. Versions 9.11 through 26.00 contain a heap out-of-bounds read of up to 3 bytes in the UDF disc image handler's File Identifier Descriptor parser. In CFileId::Parse (CPP/7zip/Archive/Udf/UdfIn.cpp), after validating size < 38 + idLen + impLen and advancing processed to 38 + impLen + idLen, the alignment-padding loop reads p[processed] while incrementing up to 3 times to reach a 4-byte boundary, and the processed <= size bounds check only runs after the loop. When (38 + impLen + idLen) % 4 != 0 and 38 + impLen + idLen == size, the loop reads 1 to 3 bytes past the end of the exact-size heap buffer allocated via buf.Alloc((size_t)item.Size). The UDF handler is registered for .iso and .udf files and auto-detected by signature, and the OOB read triggers during Open() when listing or extracting a crafted UDF image. Impact is limited to information disclosure (a 1-bit oracle per OOB byte via open/fail behavior) and denial of service (crash under hardened allocators); there is no write primitive. Version 26.01 fixes the issue.	3.1	More Details
CVE-2026-11247	Insufficient policy enforcement in CustomTabs in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-10705	A flaw has been found in dask up to 3.0. Affected by this issue is the function nunique_approx of the file dask/dataframe/hyperloglog.py of the component HLL Handler. This manipulation causes resource consumption. The attack is possible to be carried out remotely. A high degree of complexity is needed for the attack. The exploitation is known to be difficult. The pull request to fix this issue awaits acceptance.	3.1	More Details
CVE-2026-11240	Insufficient validation of untrusted input in Loader in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-45739	Strawberry GraphQL is a library for creating GraphQL APIs. In versions 0.288.4 through 0.315.3, Strawberry's bundled GraphiQL template wrote values from the GraphiQL headers editor into the browser URL query string. If a user entered a sensitive header, such as `Authorization: Bearer <token>`, the value could become visible in browser history, copied links, and server/proxy/CDN access logs after a page reload or shared request. Version 0.315.4 patches the issue.	3.1	More Details

CVE-2026-6873	An issue was discovered in Django 6.0 before 6.0.6 and 5.2 before 5.2.15. `django.http.HttpRequest.get_signed_cookie` in Django uses a non-injective salt derivation (concatenating the cookie name and salt argument), which allows a remote attacker to use a cookie in a context different from the one where it was signed, via distinct `(name, salt)` pairs that produce the same concatenation. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Peng Zhou for reporting this issue.	3.1	More Details
CVE-2026-11691	Insufficient validation of untrusted input in New Tab Page in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-11675	Out of bounds read in Skia in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-35193	An issue was discovered in Django 5.2 before 5.2.15 and 6.0 before 6.0.6. `django.middleware.cache.UpdateCacheMiddleware` in Django does not add `Authorization` to the `Vary` response header for requests bearing that header without `Cache-Control: public`, which allows remote attackers to read private cached responses via unauthenticated requests to the same URL. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Shai Berger for reporting this issue.	3.1	More Details
CVE-2026-48587	An issue was discovered in Django 5.2 before 5.2.15 and 6.0 before 6.0.6. `django.utils.cache.has_vary_header()` in Django does not strip leading or trailing whitespace from `Vary` response header values before comparison, which allows remote attackers to read cached responses via requests to URLs whose responses contain whitespace-padded Vary header values. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Navid Rezazadeh for reporting this issue.	3.1	More Details
CVE-2026-11686	Insufficient validation of untrusted input in Dawn in Google Chrome on macOS prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-7666	An issue was discovered in Django 6.0 before 6.0.6 and 5.2 before 5.2.15. `django.core.mail.backends.smtp.EmailBackend` in Django fails to prevent reuse of a partially-initialized connection after a failed `STARTTLS` handshake when `fail_silently=True`, which allows on-path network attackers to read email content via cleartext interception. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Kasper Dupont for reporting this issue.	3.1	More Details
CVE-2026-8404	An issue was discovered in Django 5.2 before 5.2.15 and 6.0 before 6.0.6. `django.middleware.cache.UpdateCacheMiddleware` in Django does not match `Cache-Control` response directives case-insensitively, which allows remote attackers to read responses that were incorrectly cached because their `Cache-Control` directives used uppercase or mixed-case values. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Ahmed Badawe for reporting this issue.	3.1	More Details
CVE-2026-11502	A weakness has been identified in JeecgBoot up to 3.9.2. Impacted is the function HttpServletResponse.sendRedirect of the file jeecg-module-system/jeecg-system-biz/src/main/java/org/jeecg/modules/system/controller/ThirdLoginController.java of the component Third-Party Login. This manipulation of the argument state causes open redirect. The attack can be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is considered difficult. The exploit has been made available to the public and could be used for attacks. The project replied: "After evaluation, this vulnerability has low exploitability in real-world scenarios: 1) Exploiting this vulnerability requires attackers to use social engineering techniques to induce victims to actively click on an OAuth login link constructed by the attacker; it cannot be triggered passively. 2) Third-party login (DingTalk/WeChat, etc.) is an optional feature and may not be enabled in most projects."	3.1	More Details
CVE-2025-52611	HCL iControl v4.0.0 was affected by Unhandled Exception - Stack Trace Disclosure vulnerability. The error occurs due to an undefined property being accessed in the application's JavaScript code. Specifically, the code attempts to read the property dashboard key from an object that is undefined. This issue likely stems from one of the following: A missing or improperly initialized object.	3.1	More Details
CVE-2025-52608	HCL iControl was affected by Missing Cookie Attributes vulnerability. It was observed that the application is missing several critical cookie attributes, including Secure and SameSite. And also path is set to root.	3.1	More Details
CVE-	A vulnerability was identified in JeecgBoot up to 3.9.2. Affected by this vulnerability is the function queryPageList of the file src\main\java\org\jeecg\modules\system\controller\SysUserController.java of the component User List Endpoint. The manipulation of the argument salt leads to information disclosure. The		More

2026-11464	attack may be initiated remotely. The attack is considered to have high complexity. The exploitation appears to be difficult. The exploit is publicly available and might be used. A fix is planned for the upcoming release.	3.1	Details
CVE-2026-11465	A security flaw has been discovered in songquanpeng one-api up to 0.6.11-preview.7. Affected by this issue is the function Redeem of the file model/redemption.go of the component Redemption Code Top-Up Endpoint. The manipulation results in business logic errors. The attack may be launched remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	3.1	More Details
CVE-2026-11684	Insufficient policy enforcement in Network in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the utility process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-11251	Insufficient policy enforcement in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-11244	Insufficient validation of untrusted input in WebAuthentication in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-9088	A flaw was found in org.keycloak.services. An administrator with delegated access to read group memberships and users can bypass user profile permissions by accessing the group members endpoint. This allows the administrator to view user attributes that are explicitly configured to be denied, leading to information disclosure.	2.7	More Details
CVE-2026-10783	A security flaw has been discovered in gradio-app gradio 6.14.0. This affects the function save_audio_to_cache of the component Audio Cache Key Handler. Performing a manipulation results in use of weak hash. The attack must be initiated from a local position. The attack is considered to have high complexity. It is indicated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The patch is named 13394. To fix this issue, it is recommended to deploy a patch.	2.5	More Details
CVE-2026-11481	A vulnerability was determined in yoanbernabeu grepai up to 0.35.0. The affected element is the function PostgresStore.LookupByContentHash of the file indexer/chunker.go of the component Postgres Embedding Cache. Executing a manipulation of the argument content_hash can lead to use of weak hash. The attack needs to be launched locally. The attack requires a high level of complexity. The exploitability is described as difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	2.5	More Details
CVE-2026-11491	A vulnerability was identified in CodeAstro Human Resource Management System 1.0. Impacted is an unknown function of the file /notice/All_notice of the component Notice Board Management. Such manipulation of the argument Notice Title with the input <svg onload="alert('Stored XSS Triggered by Ashik Mohamed')"> as part of POST leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2.4	More Details
CVE-2026-11434	A weakness has been identified in FluentCMS 0.0.5. The impacted element is an unknown function of the file /admin/blocks of the component Blocks Plugin. This manipulation 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 vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2026-11338	A security vulnerability has been detected in SourceCodester Ship Ferry Ticket Reservation System 1.0. Impacted is an unknown function of the file /admin/?page=user/manage_user. The manipulation of the argument Username leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-2026-11468	A vulnerability was detected in SourceCodester Hospitals Patient Records Management System 1.0. This issue affects some unknown processing of the file /admin/?page=room_types. Performing a manipulation of the argument room results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2026-41986	Logic bypass vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect availability.	2.4	More Details
CVE-2026-	In OpenStack Neutron before 28.0.1, a project manager can create or update a port on a shared network owned by another project and set device_owner to a value that has "network:" at the beginning ("network:dhcp" for example). The default port RBAC policies incorrectly included PROJECT_MANAGER without requiring network ownership, allowing any project manager to obtain trusted network-service	2.2	More

50266	port behavior on shared networks. Depending on backend and deployment, this can bypass anti-spoofing and security group protections, enabling DHCP, MAC, or IP spoofing against other tenants on the shared network. This is a regression of CVE-2015-5240 (OSSA-2015-018).		Details
CVE-2026-11786	A flaw was found in 389 Directory Server. The LDIF parser reads past the end of a heap buffer when processing attribute types with trailing semicolons during database import, causing an out-of-bounds read detectable under memory instrumentation.	1.9	More Details
CVE-2026-36800	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain a buffer overflow in the IPMacBindIndex parameter of the formIPMacBindDel function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36808	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the webAuthUserInfo parameter of the formAddWebAuthUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36807	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the webAuthUserPwd parameter of the formAddWebAuthUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36806	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the webAuthUserPwd parameter of the formModifyWebAuthUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36805	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain multiple buffer overflows in the Saveqqlist function via the qqStr and markStr parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36803	Shenzhen Tenda Technology Co., Ltd Tenda PW201A v1.0.5 was discovered to contain a buffer overflow in the page parameter of the qossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36802	Shenzhen Tenda Technology Co., Ltd Tenda PW201A v1.0.5 was discovered to contain a buffer overflow in the page parameter of the SafeMacFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36801	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain a buffer overflow in the IPMacBindRule parameter of the formIPMacBindAdd function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36799	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain a buffer overflow in the portalAuth parameter of the formPortalAuth function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36810	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the gotoUrl parameter of the formPortalAuth function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36798	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain multiple stack overflows in the formSetDebugCfgr function via the enable, level, and module parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36797	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain a stack overflow in the IPMacBindRuleIp parameter of the formIPMacBindModify function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36796	Shenzhen Tenda Technology Co., Ltd Tenda G0 v15.11.0.5 was discovered to contain a stack overflow in the picCropName parameter of the formCropAndSetWewifiPic function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36794	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain multiple stack overflows in the R7WebsSecurityHandler function via the username and password parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36793	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain multiple stack overflows in the formwrlSSIDset function via the mit_ssid and mis_ssid_index parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain		More

2026-36792	a stack overflow in the wl_radio parameter of the formWifiRadioSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	Details
CVE-2026-36809	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the webAuthWhiteID parameter of the formModifyWebAuthWhiteUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36811	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the picName parameter of the formDelwebAuthPic function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36784	Shenzhen Tenda Technology Co., Ltd Tenda O3 Wireless Router v1.0.0.5(4180) was discovered to contain a stack overflow in the ip parameter of the fromNetToolGet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a HTTP request.	N/A	More Details
CVE-2024-56121	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-46476	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, CustomTemplate create and update mass-assignment allows cross-workspace template takeover. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-46477	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, dataset create and update mass-assignment allows cross-workspace dataset takeover. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-46478	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, DatasetRow create and update mass-assignment allows cross-workspace row takeover. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-46479	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, evaluation create and update mass-assignment allows cross-workspace evaluation takeover. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2024-56123	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-56122	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-48488	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.4, attachment passwords are hashed using SHA-1, a cryptographically broken algorithm. SHA-1 has been vulnerable to collision attacks since 2017 (SHAttered). Version 4.1.4 fixes the issue.	N/A	More Details
CVE-2026-36813	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the picCropName parameter of the formCropAndSetWewifiPic function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2024-56120	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-49755	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in wojtekmach Req allows attacker-controlled HTTP servers to exhaust memory in a Req client via decompression-bomb response bodies. Req's default response pipeline includes Req.Steps.decode_body/1 and Req.Steps.decompress_body/1 in lib/req/steps.ex. decode_body/1 dispatches on the server-supplied content-type (or URL extension) and calls :zip.extract(body, [:memory]) for application/zip, :erl_tar.extract({:binary, body}, [:memory]) for application/x-tar, and :erl_tar.extract({:binary, body}, [:memory, :compressed]) for application/gzip / .tgz. Each returns the full decompressed archive contents as a [{name, bytes}] list in memory, with no per-entry or total size cap. decompress_body/1 walks the content-encoding header and chains :zlib/:brotli/:ezstd decoders, so a response advertising content-encoding: gzip, gzip, gzip inflates through multiple layers without bound. Both steps are enabled by default, no caller opt-in is required, and the attacker controls the content-type and content-encoding headers on their own server (or on any host reached via Req's automatic redirect following). A sub-megabyte response can expand to multiple gigabytes on the victim, crashing the BEAM process. This issue affects req: from 0.1.0 before 0.6.1.	N/A	More Details
CVE-	Shenzhen Tenda Technology Co., Ltd Tenda W20E v15.11.0.6 was discovered to contain a buffer overflow		

2026-36818	in the wewifiWhiteUserInfo parameter of the formAddWewifiWhiteUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36817	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the webAuthWhiteUserInfo parameter of the formAddWebAuthWhiteUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36816	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the wewifiWhiteUserInfo parameter of the formAddWewifiWhiteUser function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36815	Shenzhen Tenda Technology Co., Ltd Tenda W15E v15.11.0.10 was discovered to contain a buffer overflow in the hostname parameter of the formSetNetCheckTools function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36791	Shenzhen Tenda Technology Co., Ltd Tenda O3v3 v1.0.0.5 was discovered to contain a stack overflow in the save_list_data parameter of the formSetCfm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36783	Shenzhen Tenda Technology Co., Ltd Tenda O3 Wireless Router v1.0.0.5(4180) was discovered to contain a stack overflow in the domain parameter of the fromNetToolGet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-46444	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, all CRUD endpoints for OpenAI Assistants Vector Store have no authentication middleware and the route path /api/v1/openai-assistants-vector-store is not in WHITELIST_URLS. However, it is also not protected by the main auth middleware when accessed via API key — the route requires API key auth (not whitelisted), but no permission checks exist on any operation. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-40495	FOSSBilling is a free, open-source billing and client management system. Versions prior to 0.8.0 leak the exact system version through asset cache buster parameters in HTML output, bypassing the `hide_version_public` security setting. The FOSSBilling version is embedded in the query string of every `<script>` and `<link>` tag generated by the `script_tag` and `stylesheet_tag` Twig filters. This information is visible to all visitors — including unauthenticated guests — on every page, regardless of whether the `hide_version_public` setting is enabled. The `X-FOSSBilling-Version` HTTP header and the `guest.system.version` API endpoint correctly honour the `hide_version_public` setting, but the asset cache buster parameters were overlooked. Knowledge of the exact FOSSBilling version makes it significantly easier for malicious actors to identify known vulnerabilities applicable to a given installation and craft targeted exploits. While not a direct vulnerability on its own, it undermines the intended protection offered by the `hide_version_public` setting and facilitates reconnaissance. Version 0.8.0 contains a patch. There is no practical workaround that removes the version from asset URLs without modifying source code.	N/A	More Details
CVE-2026-7888	Concrete CMS below 9.5.2 is vulnerable to PHP Object Injection via unserialize() calls in the Workflow, Form block, and File/Set components that lack the allowed_classes restriction. An unauthenticated attacker may trigger arbitrary PHP object instantiation if a malicious serialized payload has been placed in the database. Thanks XananasX7 and Sanjorn Keeratirungsan (dizconnect) for both independently reporting. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 8.4 with vector CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N.	N/A	More Details
CVE-2025-55651	A NULL pointer dereference in the gf_isom_get_user_data_count function (isomedia/isom_read.c) of GPAC MP4Box v2.4 allows attackers to cause a Denial of Service (DoS) via supplying a crafted MP4 file.	N/A	More Details
CVE-2026-21032	Improper export of android application components in SmartHomeWidgetReceiver of Samsung Assistant prior to version 9.3.14 allows local attacker to execute arbitrary script.	N/A	More Details
CVE-2026-46396	HAX CMS helps manage microsite universe with PHP or NodeJs backends. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 26.0.0 due to improper sanitization of `<iframe>` elements. The application allows `javascript:` URIs in the `src` attribute, which are executed when a malicious page is viewed. This enables attackers to execute arbitrary JavaScript in the context of the victim's browser and access sensitive data exposed to client-side scripts. Version 26.0.0 fixes the issue.	N/A	More Details
CVE-2026-11764	When creating an export of all reusable media, the secrets of connected gift cards were included in the export even if the user creating the export does not have permission to view gift cards. This is inconsistent with the UI and API where only the first letters of the gift card secret are shown. Therefore, it allows circumventing a permission boundary.	N/A	More Details

CVE-2026-2638	A vulnerability in the quarantine and restore workflow of the X-VPN macOS website versions 77.0 through 77.5 allow a local attacker to leverage a race condition and symlink manipulation to achieve privileged file corruption.	N/A	More Details
CVE-2026-42061	Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.15051.93227.	N/A	More Details
CVE-2026-21034	Improper export of android application components in Samsung Auto prior to version 3.1.2.61 in Android 15 and 3.2.0.38 in Android 16 allows local attacker to change audio configuration.	N/A	More Details
CVE-2026-43924	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, the Redirect module does not validate the URL scheme of administrator-configured destination URLs before storing or issuing redirects. This allows arbitrary external URLs to be configured as redirect targets, creating an open redirect vulnerability exploitable for phishing attacks. Users following a legitimate FOSSBilling URL can be silently redirected to an attacker-controlled external site. The redirect is issued as a 301 (Moved Permanently) response, which browsers cache persistently, amplifying the impact. Exploitation requires administrator privileges to create or modify redirect entries, limiting practical attack scenarios to multi-admin environments or compromised admin accounts. Version 0.8.0 fixes the issue. Some workarounds are available. Restrict admin access to the Redirect module to trusted administrators only and/or audit existing redirect entries in the database (the `extension_meta` table with `extension = 'mod_redirect'`) for any unexpected or external target URLs.	N/A	More Details
CVE-2026-44609	Local privilege escalation due to EXE hijacking vulnerability. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.15051.93227.	N/A	More Details
CVE-2026-44682	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.15051.93227.	N/A	More Details
CVE-2026-50033	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis DeviceLock DLP (Windows) before build 9.0.15051.93227.	N/A	More Details
CVE-2026-22054	Active IQ Config Advisor version 6.7.3 contains hard-coded credentials that could allow an authenticated attacker with low privileges to perform unauthorized AutoSupport operations.	N/A	More Details
CVE-2026-22055	Active IQ OneCollect version 2.7.3 contains hard-coded credentials that could allow an authenticated attacker with low privileges to perform unauthorized AutoSupport operations.	N/A	More Details
CVE-2026-21033	Improper export of android application components in ExpressHomeWidgetReceiver of Samsung Assistant prior to version 9.3.14 allows local attacker to execute arbitrary script.	N/A	More Details
CVE-2026-36719	An information disclosure vulnerability in the /api/v1/user/info endpoint of AgentChat v2.3.0 allows unauthenticated attackers to obtain sensitive information, including SHA256 password hashes, via enumerating user IDs.	N/A	More Details
CVE-2026-36779	Shenzhen Tenda Technology Co., Ltd Tenda O3 Wireless Router v1.0.0.5(4180) was discovered to contain multiple stack overflows in the fromVirtualSer function via the puVar2, puVar1, __s2, __s1_00, and puVar3 parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-21036	Improper authorization in Samsung Internet prior to version 30.0.0.39 allows local attackers to access sensitive information.	N/A	More Details
CVE-2026-36778	Shenzhen Tenda Technology Co., Ltd Tenda O3 Wireless Router v1.0.0.5(4180) was discovered to contain a stack overflow in the username parameter of the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-36777	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain a stack overflow in the param_1 parameter of the formSetCfm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	N/A	More Details
CVE-2026-	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain a stack overflow in the Go parameter of the ask_to_reboot function. This vulnerability allows attackers to	N/A	More

36773	cause a Denial of Service (DoS) via a crafted input.		Details
CVE-2026-36772	Shenzhen Tenda Technology Co., Ltd Tenda W3 Wireless Router v1.0.0.3(2204) was discovered to contain a stack overflow in the wl_radio parameter of the formwrlSSIDget function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	N/A	More Details
CVE-2026-21037	Improper input validation in Samsung Members prior to version 5.8.01.5 allows local attackers to access arbitrary URL and launch arbitrary activity with Samsung Members privilege.	N/A	More Details
CVE-2026-49756	Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability in wojtekmach Req allows multipart parameter smuggling via attacker-influenced part metadata. Req.Utils.encode_form_part/2 in lib/req/utils.ex builds the per-part headers by interpolating the caller-supplied name, filename, and content_type values directly into the content-disposition and content-type lines with no escaping or CRLF stripping. A value containing ", \r, or \n closes the surrounding quoted value and starts a new header line; an additional \r\n--<boundary> terminates the current part and prepends a smuggled part of the attacker's choosing. This is reachable through every supported way of supplying a part. It is particularly easy when value is a %File.Stream{}, because filename then defaults to Path.basename(stream.path) and POSIX filenames may legitimately contain \r and \n. Any application that forwards user-controlled filenames (or field names / MIME types) through Req.post/2 with form_multipart: lets an attacker inject arbitrary headers into the outgoing multipart body or smuggle additional fields and parts into the request the victim service sends downstream. This issue affects req: from 0.5.3 before 0.6.0.	N/A	More Details
CVE-2026-36727	An insecure authentication vulnerability in the /api/social-sign-in endpoint of bookcars v8.3 allows attackers to bypass authentication via a forged JWT token.	N/A	More Details
CVE-2026-42840	An authenticated user can persist arbitrary HTML/JavaScript in the email_id or mobile_no fields of a Customer record and trigger unescaped rendering in the Point of Sale (POS) interface for every operator who selects that customer. This issue affects ERPNext: 16.16.0.	N/A	More Details
CVE-2026-36726	An arbitrary file deletion vulnerability in the /api/delete-temp-license/{file} endpoint of bookcars v8.3 allows unauthenticated attackers to delete arbitrary files via supplying directory traversal sequences.	N/A	More Details
CVE-2026-21035	Improper input validation in Samsung Plus TV prior to version 1.0.28.6 allows remote attackers to access sensitive information.	N/A	More Details
CVE-2026-42839	An authenticated ERPNext user with Item record edit permissions can persist arbitrary HTML/JavaScript in the item_name, description, or image fields of an Item and trigger unescaped rendering in the Point of Sale (POS) cart interface for every operator who adds that item to a transaction.This issue affects ERPNext: 16.16.0.	N/A	More Details
CVE-2026-36723	An unrestricted file rename vulnerability in the /api/create-user component of bookcars v8.3 allows authenticated attackers to leverage directory traversal sequences to move arbitrary files from temporary storage to arbitrary locations on the server filesystem. This enables unauthorized access to sensitive files, the overwriting of critical application files, and remote code execution (RCE).	N/A	More Details
CVE-2026-36722	An authenticated arbitrary file upload vulnerability in the /api/create-car-image component of bookcars v8.3 allows attackers to execute arbitrary code via uploading a crafted file.	N/A	More Details
CVE-2026-36721	A lack of cryptographic signature verification in the validateAccessToken function of bookcars v8.3 allows attackers to bypass authentication via a forged JWT token.	N/A	More Details
CVE-2026-46475	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, assistant create and update mass-assignment allows cross-workspace assistant takeover. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-46443	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, when credentials are fetched with a credentialName filter parameter, the encryptedData field is not stripped from the response. The code properly omits encryptedData when no filter is used but fails to do so when a filter is used. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Reassign nested_mmus array behind mmu_lock kvm->arch.nested_mmus[] is walked under kvm->mmu_lock, including from the MMU notifier path (kvm_unmap_gfn_range() -> kvm_nested_s2_unmap()), which can run at any time. kvm_vcpu_init_nested() reallocates the array and frees the old buffer while holding only kvm-	N/A	More Details

46317	>arch.config_lock, so such a walker can reference the freed array. Allocate the new array outside of mmu_lock, as the allocation can sleep. Under the lock, copy the existing entries, fix up the back pointers and reassign the array. Free the old buffer after dropping the lock, as kvfree() can sleep as well.		
CVE-2026-46442	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, POST /api/v1/node-custom-function lacks route-level authorization, allowing any authenticated user or API key to submit arbitrary JavaScript to the Custom JS Function node. When E2B_APIKEY is not configured — the common deployment case — Flowise executes this code inside a NodeVM sandbox. This sandbox can be escaped, allowing an attacker to reach the host process object and execute system commands via child_process. The result is authenticated remote code execution on the Flowise server host. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-46394	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, an OS command injection vulnerability exists in the Git.php library of the HAXcms PHP backend. The application constructs shell command strings using unsanitized input and executes them via proc_open(). An attacker who can control parameters passed into Git operations can execute arbitrary OS commands with the privileges of the web server. Out of 17 functions that invoke shell commands only 1 function (`commit()`) correctly uses `escapeshellarg()`. When combined with another vulnerability that allows configuration manipulation, this issue can lead to full remote code execution and complete system compromise. Version 26.0.0 patches the issue.	N/A	More Details
CVE-2026-43972	Origin Validation Error vulnerability in ninenines gun (gun_http2 module) allows cross-origin cookie injection via unvalidated HTTP/2 PUSH_PROMISE authority. In gun_http2:push_promise_frame/7, the :authority pseudo-header from an incoming PUSH_PROMISE frame is stored verbatim into the promised stream record without checking that it matches the connection's origin. When gun_http2:headers_frame/9 later processes the response headers for the promised stream, it calls gun_cookies:set_cookie_header/7 with the unvalidated server-supplied authority before any status branching and before user code can act. This violates RFC 7540 §10.6 / RFC 9113 §8.4, which require receivers to treat as a protocol error any push for a resource the server is not authoritative for. A malicious or compromised HTTP/2 server can plant cookies scoped to arbitrary third-party domains into the client's shared cookie store. This enables session fixation attacks against those domains and, if the planted cookie overrides a legitimate session token, may result in account takeover. No user interaction beyond making a normal HTTP/2 request to the attacker-controlled server is required. This issue affects gun: from 2.0.0 before 2.4.0.	N/A	More Details
CVE-2026-43973	Uncontrolled Resource Consumption vulnerability in ninenines gun (gun_http module) allows a malicious server to exhaust client memory via unbounded HTTP/1.1 response buffering. In gun_http:handle/5, three clauses accumulate incoming TCP data into the connection's buffer field using binary concatenation with no upper-bound check: the head clause appends data until the \r\n\r\n header terminator is found; the body_chunked clause appends data whenever cow_http_te:stream_chunked/2 returns a more result indicating an incomplete chunk boundary; and the body_trailer clause appends data until the trailing \r\n\r\n is found. In each case, when the expected terminator never arrives, the enlarged binary is stored back into state and the process waits for more data, with no configurable or hard-coded ceiling on buffer size. A malicious or compromised server can exploit this by sending a partial response that never completes. For example, a response may begin with HTTP/1.1 200 OK\r\nX-Pad: followed by an unbounded stream of arbitrary bytes, never sending the header terminator. The gun connection process will continuously append the incoming data to its buffer, causing unbounded heap growth. Because BEAM imposes no per-process heap limit by default, a single malicious connection can exhaust all available memory on the node, causing a node-wide out-of-memory crash. This issue affects gun: from 1.0.0 before 2.4.0.	N/A	More Details
CVE-2026-43974	Unexpected Status Code or Return Value vulnerability in ninenines gun (gun_http module) allows a malicious HTTP server to force the client into raw protocol mode via an unsolicited 101 Switching Protocols response. In gun_http:handle_inform/8, when a 101 Switching Protocols response is received over HTTP/1.1, the function verifies only that the Upgrade header is syntactically valid and that the stream reference is a plain reference(). It does not check whether the client ever sent an Upgrade or Connection: upgrade header on the corresponding request. Because this check is absent, any 101 response (solicited or not) causes gun to dispatch a gun_upgrade message to the caller and transition the entire connection to raw protocol mode. A malicious or compromised HTTP server can send an unsolicited 101 response to any HTTP/1.1 request, causing the gun client to abandon HTTP framing for that connection. Once in raw mode, gun_raw applies no flow control (flow=infinity) and re-arms socket active mode after every received packet, so the server can flood the client with arbitrary bytes. These are forwarded as unbounded gun_data messages to the owner process, exhausting its mailbox and BEAM memory, ultimately crashing the VM. This issue affects gun: from 2.0.0 before 2.4.0.	N/A	More Details
CVE-2026-10729	An HTML injection vulnerability in the notification email for "Slow Redirect" and "Cloned Website" Canarytokens exists in Thinkst Applied Research Canarytokens, enabling Interface Manipulation, Cross-Site Scripting (XSS) in emails clients that render HTML emails. This issue affects Canarytokens: from Docker tag sha-c42435e before sha-bfda4df, from Git commit c42435e before bfda4df.	N/A	More Details

CVE-2026-11346	A Server-Side Request Forgery (SSRF) vulnerability in the custom process creation feature of linqi allows an authenticated attacker to probe internal network components. By crafting a specific process containing an HTTP Request component, an attacker can force the server to send arbitrary HTTP requests. By observing the varying application responses (Success, Failed, or 504 Gateway Time-out), the attacker can determine the status of internal ports, leading to internal network reconnaissance.	N/A	More Details
CVE-2026-49232	Routinator exits on any error when accepting incoming HTTP or RTR connections, including ones it can recover from such as running out of file descriptors. This condition can be triggered maliciously by an attacker by opening a large number of connections to the HTTP or RTR server. This only affects users that make their HTTP or RTR server available to untrusted networks.	N/A	More Details
CVE-2026-49233	Routinator does not properly check the module component of rsync URIs, which are used to create the file system paths for the Routinator cache. This allows for path traversal by having a module name containing .., potentially providing an attacker access to the entire Routinator rsync cache.	N/A	More Details
CVE-2026-49234	When sending a specifically crafted non-UTF-8 string as select-asn query parameter to the /api/v1/origins endpoint, Routinator crashes. This only affects users who allow API access from untrusted networks.	N/A	More Details
CVE-2026-11607	Backend users with access to the Form Framework were able to use files not ending in .form.yaml as form definitions, which were processed without denying the incorrect file extension. Maliciously crafted form definition files can be used to execute arbitrary SQL statements, allowing attackers to escalate privileges by creating administrative backend user accounts. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.51, 12.0.0-12.4.46, 13.0.0-13.4.31 and 14.0.0-14.3.3.	N/A	More Details
CVE-2026-47343	Non-privileged backend users with file mount access were able to perform write operations (move, delete, rename) on folders representing the root of an active file mount due to missing authorization restrictions. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0 through 11.5.50, 12.0.0 through 12.4.45, 13.0.0 through 13.4.30, and 14.0.0 through 14.3.2.	N/A	More Details
CVE-2026-49235	When Routinator encounters a file via RRDP using a specifically crafted Document Type Definition, Routinator crashes.	N/A	More Details
CVE-2026-47324	ProjectsAndPrograms school-management-system is vulnerable to Stored Cross-Site Scripting (XSS) in multiple attributes of students and teachers objects. An authorized attacker (e.g., a teacher or administrator) can inject malicious JavaScript that is subsequently executed in other users' browsers. Critically, when chained with CVE-2025-11661, which allows unauthenticated access to backend endpoints, this vulnerability can be exploited by a remote attacker without privileges to inject and execute arbitrary JavaScript. The maintainers were notified early about this vulnerability but did not provide details regarding affected versions. The version corresponding to commit 6b6fae5 was tested and confirmed vulnerable; other versions were not tested and may also be affected.	N/A	More Details
CVE-2026-47325	ProjectsAndPrograms school-management-system uses predictable credentials by generating student's and teacher's passwords solely from the user's date of birth (e.g., 12072000 for 12 July 2000). The application does not require or prompt users to change the password upon first login. This behavior allows attackers to easily guess or derive valid credentials, leading to unauthorized account access. The maintainers were notified early about this vulnerability but did not provide details regarding affected versions. The version corresponding to commit 6b6fae5 was tested and confirmed vulnerable; other versions were not tested and may also be affected.	N/A	More Details
CVE-2026-47346	Backend users with file write permissions were able to upload form definition files with mixed-case extensions (e.g., .FORM.YAML) to bypass the Form Framework's upload restriction. Maliciously crafted form definition files can be used to execute arbitrary SQL statements, allowing attackers to escalate privileges by creating administrative backend user accounts. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.50, 12.0.0-12.4.45, 13.0.0-13.4.30 and 14.0.0-14.3.2.	N/A	More Details
CVE-2026-10731	SQL injection in the 'two_steps_auth_code' parameter processed by the 'twoStepsAuthVerification' function within the '/user-login' endpoint. The two-factor authentication (2FA) functionality can be accessed without prior authentication, allowing unauthenticated attackers to execute arbitrary SQL queries on the backend database. A successful exploit could lead to database enumeration, the unauthorised creation of privileged users, the modification or deletion of critical information, and denial-of-service conditions.	N/A	More Details
CVE-2026-10238	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-44963	A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user.	N/A	More Details

CVE-2026-50052	In Vinyl Cache before 9.0.1 and Varnish Cache before 9.0.3, a deficiency in HTTP/2 request parsing can be exploited to launch a backend request desync attack (request smuggling), which in turn can be used for cache poisoning, authentication bypass, or possibly even information disclosure and manipulation. The attack vector only exists if HTTP/2 support is enabled by setting the feature parameter to contain +http2. HTTP/2 support is disabled by default.	N/A	More Details
CVE-2026-6209	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-41539	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3492 build 20260507 and later QuTS hero h5.2.9.3499 build 20260514 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3500 build 20260520 and later	N/A	More Details
CVE-2025-62858	A buffer overflow 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 modify memory or crash processes. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3397 build 20260206 and later	N/A	More Details
CVE-2026-8714	A denial-of-service vulnerability exists in the RTSP server component of TP-Link Tapo C520WS v2 due to improper handling of syntactically invalid input. Crafted inputs can trigger a processing error, causing the RTSP service to enter non-responsive state. Successful exploitation may cause the RTSP in a denial-of-service condition.	N/A	More Details
CVE-2026-6208	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-6207	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-44083	An authorization bypass through user-controlled key vulnerability has been reported to affect QuMagie. The remote attackers can then exploit the vulnerability to gain unintended privileges. We have already fixed the vulnerability in the following version: QuMagie 2.9.1 and later	N/A	More Details
CVE-2026-11369	The Comment API (GET /api/Comment and POST /api/Comment) in the affected application fails to perform authorization checks to verify that the requesting user has access to the object identified by the relatedObjectId. This Insecure Direct Object Reference (IDOR) vulnerability allows any authenticated user to read and write comments on any process across all business units by supplying an arbitrary object GUID.	N/A	More Details
CVE-2025-41259	SWUpdate before 2026.05 is affected by a time-of-check time-of-use (TOCTOU) race condition that allows local unprivileged attackers to escalate privileges to root or install untrusted contents using a signed update.	N/A	More Details
CVE-2026-46390	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Starting in version 2.0.0 and prior to version 26.0.0, the gitlist plugin is exposed to unauthenticated users, allowing unauthenticated browsing of git repositories and git history. Version 26.0.0 patches the issue.	N/A	More Details
CVE-2026-46315	In the Linux kernel, the following vulnerability has been resolved: io_uring/waitid: clear waitid info before copying it to userspace IORING_OP_WAITID stores its result fields in struct io_waitid::info and later copies them to userspace siginfo. The prep path initializes the request arguments, but it does not initialize info itself. If the wait operation completes without reporting a child event, the common wait code can return without writing wo_info. In that case io_waitid_finish() still copies iw->info to userspace, exposing stale bytes from the reused io_kiocb command storage. Clear the result storage during prep so the io_uring path matches the regular waitid syscall, which uses a zero-initialized struct waitid_info.	N/A	More Details
CVE-2026-46391	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Starting in version 9.0.1 and prior to version 26.0.0 of @haxtheweb/open-apis, multiple functions conduct substring-only matching to validate hostnames to which basic authorization should be sent. An attacker can append the matched substrings to an attacker-controlled endpoint and capture authentication. Version 26.0.0 fixes the issue.	N/A	More Details
CVE-2026-46393	HAX CMS helps manage microsite universe with PHP or NodeJs backends. An authenticated Server-Side Request Forgery (SSRF) vulnerability in versions prior to 26.0.0 allows authenticated users to fetch arbitrary internal or local resources and write the responses to a web-accessible directory, enabling arbitrary file read and internal network access. Version 26.0.0 contains a fix.	N/A	More Details

CVE-2026-38500	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-47347	Applications that use GeneralUtility::sanitizeLocalUrl to allow only local URLs are vulnerable to open redirect attacks if the URL is used after it has passed the aforementioned sanitization checks. This enables attackers to redirect users to external content and carry out phishing attacks. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.50, 12.0.0-12.4.45, 13.0.0-13.4.30 and 14.0.0-14.3.2.	N/A	More Details
CVE-2026-47348	Editors with access to create or modify page content were able to include HTML markup in page titles that were stored in the search index without sanitization. When displayed in frontend search results via the Indexed Search plugin, these titles were rendered without proper output encoding, resulting in a Cross-Site Scripting vulnerability. This issue affects TYPO3 CMS versions 13.0.0-13.4.30 and 14.0.0-14.3.2.	N/A	More Details
CVE-2026-47349	Backend users with access to the Recycler module were able to restore soft-deleted records on pages or for tables they were not authorized to modify. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.51, 12.0.0-12.4.46, 13.0.0-13.4.31 and 14.0.0-14.3.3.	N/A	More Details
CVE-2026-8914	In Teltonika Networks RUTOS devices, running versions 7.22 through 7.23.2 and TSWOS devices running versions 1.09 through 1.09.1, due to unsafe calls to an eval function in rpc-profile, a vulnerability exists where a lower privileged user could perform command injection as the root user.	N/A	More Details
CVE-2026-42863	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, a mass assignment vulnerability exists in the chatflow update endpoint of FlowiseAI. The endpoint allows clients to modify server-controlled properties such as deployed, isPublic, workspaceId, createdDate, and updatedDate when updating a chatflow object. Due to missing server-side validation and authorization checks, an authenticated user can manipulate internal attributes of a chatflow and reassign it to another workspace. This allows cross-workspace resource reassignment and unauthorized modification of deployment and visibility settings. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-9506	This vulnerability exists in Bagisto due to improper validation of user-supplied input in the ImageCacheController component. An unauthenticated remote attacker could exploit this vulnerability by sending crafted path traversal sequences through the filename parameter to access arbitrary files outside the intended directory on the targeted system. Successful exploitation of this vulnerability could allow an attacker to read arbitrary sensitive files on the targeted system.	N/A	More Details
CVE-2026-11799	UXSS in Focus for iOS / Klar Webkit navigation. This vulnerability was fixed in Focus for iOS 151.3.1 and Klar for iOS 151.3.1.	N/A	More Details
CVE-2026-11345	An Improper Authentication vulnerability in the /api/Cdn/GetFile endpoint of linqi allows unauthenticated, remote attackers to bypass file access controls. The ValidateAnonFileAccess function incorrectly grants access if an 'AnonFile' query parameter containing exactly 256 characters is provided. While this flaw allows bypassing the intended authorization check, the actual security impact is negligible; the exposed resources are strictly limited to minified JavaScript and CSS files that contain no sensitive data and are already publicly accessible via a standard CDN.	N/A	More Details
CVE-2026-6445	A flaw exists in FlashArray Purity where insufficient filtering of certain data paths could expose sensitive information to an authenticated user with low privileges.	N/A	More Details
CVE-2026-6444	A flaw exists in the FlashArray Purity management interface where an authenticated low-privileged user may, under specific conditions, access functionality beyond their assigned privileges.	N/A	More Details
CVE-2026-46395	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, the `hmacBase64()` function in the HAXcms Node.js backend contains two critical cryptographic implementation errors that together allow any unauthenticated attacker to extract the system's private signing key and forge arbitrary admin-level JSON Web Tokens (JWTs) allowing them to get full admin access with a single HTTP request. First, the function passes the literal string "0" as the HMAC signing key instead of the key parameter, making every HAXcms instance compute identical HMACs for the same input. Then, after computing the HMAC, the function concatenates the real key parameter which is "this.privateKey + this.salt", the system's master signing secret is directly onto the output. The combined buffer is base64-encoded and returned as the token. Every base64url token produced has the same structure: 32 bytes HMAC keyed with "0" and N bytes of `privateKey+salt`. An attacker base64-decodes any token, discards the first 32 bytes, and reads the private key directly. The `/system/api/connectionSettings` endpoint is unauthenticated and returns multiple tokens generated by this function. A single GET request to this endpoint exposes the private key. The PHP backend implements this function correctly with the actual key and returns only the hash. The PHP version	N/A	More Details

	produces 44-character tokens whereas the broken Node.js version produces 139+ character tokens. Version 26.0.0 fixes the issue.		
CVE-2026-49741	Backend users with write access to the form_definition database table were able to directly create, update, or delete form definition records via DataHandler, bypassing the Form Framework's persistence validation and permission checks. This allowed injecting arbitrary form configurations, re-enabling attack vectors originally addressed in TYPO3-CORE-SA-2018-003, including SQL injection and privilege escalation. This issue affects TYPO3 CMS versions 14.0.0-14.3.3.	N/A	More Details
CVE-2026-50265	Rejected reason: This CVE ID was assigned as a duplicate of CVE-2026-50292	N/A	More Details
CVE-2026-21038	Improper input validation in Samsung Android USB Driver for Windows prior to version 1.9.5.0 allows local attacker to access out-of-bounds memory.	N/A	More Details
CVE-2026-46274	In the Linux kernel, the following vulnerability has been resolved: io-wq: check that the predecessor is hashed in io_wq_remove_pending() io_wq_remove_pending() needs to fix up wq->hash_tail[] if the cancelled work was the tail of its hash bucket. When doing this, it checks whether the preceding entry in acct->work_list has the same hash value, but never checks that the predecessor is hashed at all. io_get_work_hash() is simply atomic_read(&work->flags) >> IO_WQ_HASH_SHIFT, and the hash bits are never set for non-hashed work, so it returns 0. Thus, when a hashed bucket-0 work is cancelled while a non-hashed work is its list predecessor, the check spuriously passes and a pointer to the non-hashed io_kiocb is stored in wq->hash_tail[0]. Because non-hashed work is dequeued via the fast path in io_get_next_work(), which never touches hash_tail[], the stale pointer is never cleared. Therefore, after the non-hashed io_kiocb completes and is freed back to req_cachep, wq->hash_tail[0] is a dangling pointer. The io_wq is per-task (tctx->io_wq) and survives ring open/close, so the dangling pointer persists for the lifetime of the task; the next hashed bucket-0 enqueue dereferences it in io_wq_insert_work() and wq_list_add_after() writes through freed memory. Add the missing io_wq_is_hashed() check so a non-hashed predecessor never inherits a hash_tail[] slot.	N/A	More Details
CVE-2026-46275	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_uart: fix UAFs and race conditions in close and init paths Vulnerabilities leading to Use-After-Free (UAF) and Null Pointer Dereference (NPD) conditions were observed in the lifecycle management of hci_uart. The primary issue arises because the workqueues (init_ready and write_work) are only flushed/cancelled if the HCI_UART_PROTO_READY flag is set during TTY close. If a hangup occurs before setup completes, hci_uart_tty_close() skips the teardown of these workqueues and proceeds to free the `hu` struct. When the scheduled work executes later, it blindly dereferences the freed `hu` struct. Furthermore, several data races and UAFs were identified in the teardown sequence: 1. Calling hci_uart_flush() from hci_uart_close() without effectively disabling write_work causes a race condition where both can concurrently double-free hu->tx_skb. This happens because protocol timers can concurrently invoke hci_uart_tx_wakeup() and requeue write_work. 2. Calling hci_free_dev(hdev) before hu->proto->close(hu) causes a UAF when vendor specific protocol close callbacks dereference hu->hdev. 3. In the initialization error paths, failing to take the proto_lock write lock before clearing PROTO_READY leads to races with active readers. Additionally, hci_uart_tty_receive() accesses hu->hdev outside the read lock, leading to UAFs if the initialization error path frees hdev concurrently. Fix these synchronization and lifecycle issues by: 1. Re-ordering hci_uart_tty_close() to clear HCI_UART_PROTO_READY first, followed immediately by a cancel_work_sync(&hu->write_work). Clearing the flag locks out concurrent protocol timers from successfully invoking hci_uart_tx_wakeup(), effectively rendering the cancellation permanent and preventing the tx_skb double-free. 2. Note: Clearing PROTO_READY early causes hci_uart_close() to skip hu->proto->flush(). This is perfectly safe in the tty_close path because hu->proto->close() executes shortly after, which intrinsically purges all protocol SKB queues and tears down the state. 3. Relocating hu->proto->close(hu) strictly prior to hci_free_dev(hdev) across all close and error paths to prevent vendor-level UAFs. 4. Moving the hdev->stat.byte_rx increment in hci_uart_tty_receive() inside the proto_lock read-side critical section to safely synchronize with device unregistration. 5. Adding cancel_work_sync(&hu->write_work) to hci_uart_close() to safely flush the workqueue before hci_uart_flush() is invoked via the HCI core. 6. Utilizing cancel_work_sync() instead of disable_work_sync() across all paths to prevent permanently breaking user-space retry capabilities.	N/A	More Details
CVE-2026-46440	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, the checkBasicAuth endpoint validates credentials in plaintext without rate limiting and with direct comparison. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-46441	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, a mass assignment vulnerability exists in the assistant update endpoint of FlowiseAI. The endpoint allows authenticated users to modify server-controlled properties such as workspaceId, createdDate, and updatedDate when updating an assistant resource. Due to missing server-side validation and authorization checks, an attacker can manipulate the workspaceId field and reassign assistants to arbitrary workspaces. This breaks tenant isolation in multi-workspace environments. This issue has been	N/A	More Details

	patched in version 3.1.2.		
CVE-2026-49742	Backend users with file download permissions were able to download files from the fallback storage of the file abstraction layer (FAL) via the Media Module. Since the fallback storage resolves paths relative to the server's document root, this could expose sensitive files such as log files. This issue affects TYPO3 CMS versions 11.0.0-11.5.50, 12.0.0-12.4.45, 13.0.0-13.4.30 and 14.0.0-14.3.2.	N/A	More Details
CVE-2026-42862	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, a mass assignment vulnerability exists in the tool update endpoint of FlowiseAI. The endpoint allows authenticated users to modify server-controlled properties such as workspaceId, createdDate, and updatedDate when updating a tool resource. Due to missing server-side validation and authorization checks, an attacker can manipulate the workspaceId field and reassign tools to arbitrary workspaces. This breaks tenant isolation in multi-workspace environments. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-47350	Backend users were able to move records to a different page without having edit permissions on the source page. This issue affects TYPO3 CMS versions 13.0.0-13.4.31 and 14.0.0-14.3.3.	N/A	More Details
CVE-2026-47430	## Summary The iOS implementation of `cordova-plugin-inappbrowser` passes the `id` field from a `WKScriptMessage` body to `commandDelegate sendPluginResult:callbackId:` with no format validation (`CDVWKInAppBrowser.m:560–574`). Any web content loaded inside the InAppBrowser can fire any pending Cordova callback in the host app by posting a message whose `id` field is a guessable or enumerated callback identifier. An attack abusing this weakness must be tailored to the specific plugins and callback IDs the host app uses. Though an attacker with knowledge of common Cordova plugin configurations could craft reusable payloads targeting widely-adopted plugins. ## Impact An unauthenticated remote attacker who controls content displayed in the InAppBrowser — via a URL the app opens (OAuth redirect, marketing link, deep-link target) or a network interception — can call `window.webkit.messageHandlers.cordova_iab.postMessage({id: '<victim-callback-id>', d: '...'})` to fire callbacks belonging to any other installed Cordova plugin (Camera, Contacts, File, Geolocation). Cordova callback IDs follow the predictable format `<PluginName><sequential-integer>`, making enumeration feasible. Successful exploitation allows the attacker to spoof plugin results across trust boundaries — for example, injecting a forged camera approval, a fabricated contacts list, or a crafted file-read response. This issue affects Cordova Plugin InAppBrowser: from 3.1.0 through 6.0.0. Users are recommended to upgrade to version 6.0.1, which fixes the issue.	N/A	More Details
CVE-2022-31114	backpack/crud provides Create, Read, Update & Delete (CRUD) functions for Backpack, a collection of Laravel packages that help users build custom administration panels. Versions prior to 5.0.13, 4.1.69, and 4.0.63 are vulnerable to cross-site scripting. An attacker could conduct a targeted phishing campaign, in order to trick users or admins into clicking a malicious link, which under very specific circumstances could give them information or possibly admin access. Versions 5.0.13, 4.1.69, and 4.0.63 patch the issue. As a workaround, manually look inside error views in `resources/views/errors` and output `e($exception->getMessage())` instead of `$exception->getMessage()`.	N/A	More Details
CVE-2026-3276	unicodedata.normalize() can take excessive CPU time when processing specially crafted Unicode input containing long runs of combining characters with alternating Canonical Combining Class values. This affects all normalization forms.	N/A	More Details
CVE-2026-42317	GLPI is a free asset and IT management software package. Starting in version 0.78 and prior to versions 10.0.25 and 11.0.7, a technician can delete arbitrary files from the filesystem as long as the webserver has write rights on them. Upgrade to 10.0.25 or 11.0.7 to receive a patch.	N/A	More Details
CVE-2025-71315	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Convert to DRM's vblank timer Replace vkms' vblank timer with the DRM implementation. The DRM code is identical in concept, but differs in implementation. Vblank timers are covered in vblank helpers and initializer macros, so remove the corresponding hrtimer in struct vkms_output. The vblank timer calls vkms' custom timeout code via handle_vblank_timeout in struct drm_crtc_helper_funcs.	N/A	More Details
CVE-2026-47351	Backend users were able to insert arbitrary records and files into the TYPO3 clipboard without proper read permission checks, which allowed users to gather information about records and files they were not authorized to view. This issue affects TYPO3 CMS versions 10.4.0-13.4.30 and 14.0.0-14.3.2.	N/A	More Details
CVE-2026-47352	Authenticated backend users were able to retrieve file metadata via several Backend API routes without proper permission checks, allowing access to files outside their permitted file mounts or storages. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.51, 12.0.0-12.4.46, 13.0.0-13.4.31 and 14.0.0-14.3.3.	N/A	More Details
CVE-2026-42318	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to versions 10.0.25 and 11.0.7, low privilege users with access to planning can delete any object in GLPI. Upgrade to 11.0.7 or 10.0.25 to receive a patch. As a workaround, disable delete rights for User's planning.	N/A	More Details

CVE-2026-42861	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to version 3.1.2, a mass assignment vulnerability exists in the variable update endpoint of FlowiseAI. The endpoint allows authenticated users to modify server-controlled properties such as workspaceId, createdDate, and updatedDate when updating a variable resource. Due to missing server-side validation and authorization checks, an attacker can manipulate the workspaceId field and reassign variables to arbitrary workspaces. This behavior may break tenant isolation in multi-workspace environments. This issue has been patched in version 3.1.2.	N/A	More Details
CVE-2026-42320	GLPI is a free asset and IT management software package. Starting in version 0.50 and prior to versions 10.0.25 and 11.0.7, a technician can read arbitrary files inside the GLPI_DOC_DIR. Upgrade to 10.0.25 or 11.0.7 to receive a patch.	N/A	More Details
CVE-2026-42321	GLPI is a free asset and IT management software package. Starting in version 10.0.4 and prior to version 10.0.25, a technician can store an XSS payload in the asset locked tab. Upgrade to 10.0.25 or 11.0.7 to receive a patch.	N/A	More Details
CVE-2026-44281	GLPI is a free asset and IT management software package. Starting in version 0.78 and prior to versions 10.0.25 and 11.0.7, an authenticated user with config READ permission can read a specific asset object. Upgrade to 11.0.7 or 10.0.25 to receive a patch.	N/A	More Details
CVE-2026-6657	A vulnerability in jupyter-server versions 1.12.0 through 2.17.0 allows an attacker to bypass CORS origin validation when the `allow_origin_pat` configuration is used. The issue arises from the use of `re.match()` for validating the `Origin` header, which only anchors at the start of the string. This allows attacker-controlled domains such as `trusted.example.com.evil.com` to pass validation against patterns intended to match `trusted.example.com`. The vulnerability affects multiple locations in the codebase, including CORS headers, WebSocket connections, referer validation, and login redirects, potentially enabling phishing attacks, arbitrary code execution, and unauthorized access to sensitive API responses.	N/A	More Details
CVE-2026-49738	The path allowance check in GeneralUtility::isAllowedAbsPath() performed a plain string prefix comparison without requiring a directory separator boundary, causing a path like /var/www/html-other/secret.yaml to be incorrectly accepted as valid when the project root was /var/www/html. Administrator users with access to the File Abstraction Layer were able to create new file storage definitions pointing to directories outside the project root, bypassing this path check. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.51, 12.0.0-12.4.46, 13.0.0-13.4.31 and 14.0.0-14.3.3.	N/A	More Details
CVE-2026-49740	TYPO3's cache frontend (VariableFrontend) and persistent key-value store (Registry) deserialized PHP payloads without integrity validation or class restrictions. An attacker with write access to the underlying storage backend (cache store or sys_registry database table) could inject a crafted serialized payload to trigger PHP Object Injection, potentially exploiting a gadget chain to achieve Remote Code Execution or other high-impact effects. Exploiting this vulnerability requires direct local write access to the storage, such as the SQL database or file system. This issue affects TYPO3 CMS versions before 10.4.57, 11.0.0-11.5.51, 12.0.0-12.4.46, 13.0.0-13.4.31 and 14.0.0-14.3.3.	N/A	More Details
CVE-2026-46316	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic-its: Drop the translation cache reference only for the erased entry vgic_its_invalidate_cache() walks the per-ITS translation cache with xa_for_each() and drops the cache's reference on each entry with vgic_put_irq(). It puts the iterated pointer, though, rather than the value returned by xa_erase(). The function is called from contexts that do not exclude one another: the ITS command handlers hold its_lock, the GITS_CTLR write path holds cmd_lock, and the path that clears EnableLPIs in a redistributor's GICR_CTLR holds neither. Two or more of them can drain the same cache concurrently, and if each one observes the same entry, erases it and then puts it, the single reference the cache holds on that entry is dropped more than once. The entry can then be freed while an ITE still maps it. xa_erase() is atomic and returns the previous entry, so put only the entry that this context actually removed. The cache reference is then dropped exactly once per entry even when the invalidations run concurrently, and the behavior is unchanged when only one context runs.	N/A	More Details
CVE-2026-2596	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-45287	OpenTelemetry-Go is the Go implementation of OpenTelemetry. Prior to version 0.0.17, `go.opentelemetry.io/otel/schema/v1.0` and `go.opentelemetry.io/otel/schema/v1.1` leaks one file descriptor on each successful `ParseFile` call. `ParseFile` opens the schema file and passes it to `Parse` without closing it; repeated parsing in a long-running process can exhaust the process file descriptor limit and cause denial of service. Exploitation depends on a consuming application exposing repeated schema parsing to an attacker-controlled path. Version 0.0.17 contains a patch for the issue.	N/A	More Details
	Two path traversal vulnerabilities in the Network Installation Service (NIS) of Altium Enterprise Server allow an unauthenticated network attacker to write arbitrary files to any writable location on the server filesystem and to read package archive files from the server. No authentication, session, or credentials		

CVE-2026-11420	are required. Because content-controlled files can be written to web-accessible directories, or used to overwrite application binaries or configuration files, exploitation can be escalated to remote code execution in the context of the service account, and can disclose deployment package contents. Altium 365 cloud deployments are not affected, as the Network Installation Service is not part of the cloud offering.	N/A	More Details
CVE-2026-0420	An improper implementation of TLS certificate validation vulnerability found in ReadyCloud client app which can allow an attacker to perform attacker-in-the-middle (MiTM) style attacks impacting product's confidentiality. This vulnerability affects the listed NETGEAR models.	N/A	More Details
CVE-2026-48907	A vulnerability in the JCE editor extension for Joomla allows the creation of new editor profiles for unauthenticated users, ultimately resulting in PHP code upload and execution.	N/A	More Details
CVE-2026-21837	HCL Digital Experience is affected by an OS command injection vulnerability in the Digital Asset Management API. An attacker may execute arbitrary operating system commands, typically inheriting the privileges of the vulnerable application, which could possibly lead to a complete system takeover and data compromise.	N/A	More Details
CVE-2026-35058	Improper validation of packet length during tls-crypt-v2 key extraction in OpenVPN 2.6.0 through 2.6.19 and 2.7_alpha1 through 2.7.1 allows authenticated attackers to trigger a fatal assertion and cause a denial of service via a specially crafted packet.	N/A	More Details
CVE-2026-46511	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, an attack chain utilizing Stored XSS alongside dynamic token exposure in the `/system/api/connectionSettings` endpoint allows an authenticated attacker to perform a complete cross-tenant account takeover. The API dynamically leaks the active session's authentication tokens (including the `jwt`, `user_token`, `site_token`, and `appstore_token`) into a global JavaScript variable (`window.appSettings`). An attacker can exploit the XSS vulnerability to force a victim's browser to silently fetch their specific connection settings, extract the tokens, and exfiltrate them to an attacker-controlled webhook. Version 26.0.0 patches the issue.	N/A	More Details
CVE-2026-47344	When ALLOW_INSECURE_RAW_TEXT is enabled, whitespace-variant closing tags (e.g., </style\t>) are not recognized by the sanitizer but accepted by browsers as valid end tags, allowing subsequent content to escape sanitization. This allows bypassing the cross-site scripting prevention mechanism of typo3/html-sanitizer before version 2.3.2.	N/A	More Details
CVE-2026-47345	Namespace attributes are not encoded correctly during HTML serialization. This allows bypassing the cross-site scripting prevention mechanism of typo3/html-sanitizer before version 2.3.2.	N/A	More Details
CVE-2026-11414	A hard-coded cryptographic key is used by Altium Enterprise Server to sign file download URLs in the Vault service. Because the key is identical across all installations, an unauthenticated network attacker who can reach the server can forge valid download signatures and retrieve files from the Vault storage area without any authentication, session, or credentials. A separate path traversal vulnerability in the same download endpoint allows the configured storage root to be escaped, enabling reads of arbitrary files on the server filesystem. Combined, these issues allow an unauthenticated attacker to obtain sensitive server configuration and key material, which can lead to full server compromise. The vulnerability can be chained with CVE-2026-9152 to enumerate and bulk-download stored content. Altium 365 cloud deployments are not impacted in practice, as file storage uses object storage rather than the local filesystem.	N/A	More Details
CVE-2026-11419	A path traversal vulnerability exists in the Altium Enterprise Server Vault Service UploadController due to improper validation of a user-controlled path component in image upload requests. An authenticated user can supply a crafted absolute path so that the configured storage root is discarded, allowing arbitrary files to be written to any location on the server filesystem writable by the service account. Because content-controlled files can be written to web-accessible directories, or used to overwrite application binaries or configuration files, this can be escalated to remote code execution, service takeover, or denial of service. Altium 365 cloud deployments are not affected, as the affected endpoint is not reachable and the cloud storage architecture mitigates the file-write primitive.	N/A	More Details
CVE-2026-40215	A race condition in OpenVPN 2.6.0 through 2.6.19 and 2.7_alpha1 through 2.7.1 allows remote attackers to potentially cause a server crash or leak heap memory via a use-after-free triggered during TLS session promotion.	N/A	More Details
CVE-2026-44541	Fides is an open-source privacy engineering platform. From version 2.33.0 to before version 2.84.5, there is a DOM-based XSS vulnerability in fides.js via the fides_description override. This issue has been patched in version 2.84.5.	N/A	More Details
	bz2.BZ2Decompressor objects could be reused after a decompression error. If an application caught the		

CVE-2026-9669	resulting OSError and retried with the same decompressor, crafted input could cause the decompressor to resume from an invalid internal state and perform out-of-bounds writes to a stack buffer. This could crash the process when processing untrusted data.	N/A	More Details
CVE-2026-34181	Issue Summary: The PKCS#12 file processing fails to perform sufficient input validation for files that use Password-Based Message Authentication Code 1 (PBMAC1) integrity mechanism allowing a certificate and private key forgery. Impact Summary: An attacker impersonating a user can cause a service reading PKCS#12 files to accept forged certificates and private keys with a 1 in 256 probability. If a service accepting PKCS#12 files is using passwords for authenticating the received files, the attacker can create unencrypted PKCS#12 files that use PBMAC1 authentication that specifies an HMAC key of only one byte, allowing them to craft a file that will be accepted with a 1 in 256 probability. That would then cause the service to accept a certificate and private key controlled by the attacker. The FIPS modules are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	N/A	More Details
CVE-2026-34182	Issue Summary: Cryptographic Message Services (CMS) processing fails to perform sufficient input validation on the cipher and tag length fields of AuthEnvelopedData containers, leading to various potential compromises. Impact Summary: Attackers making use of these vulnerabilities may achieve key-equivalent functionality for a given CMS recipient and/or bypass integrity validation for a given message. In one use case, an attacker may send a CMS message containing AuthEnvelopedData with the cipher specified as a non-AEAD cipher. OpenSSL erroneously allows this selection, and attempts to decrypt and validate the message. An on-path attacker who captures one legitimate AES-GCM AuthEnvelopedData addressed to the victim can re-emit it with the recipientInfos set left byte-for-byte intact, so the victim's private key still unwraps the genuine CEK (the content-encryption key), but with the inner OID rewritten to AES-256-OFB (Output Feedback Mode, an unauthenticated keystream mode) and with an attacker-chosen IV and ciphertext. The victim initializes AES-256-OFB under the real CEK, never consults the MAC field, and CMS_decrypt() returns success. If the application under attack responds to the attacker with any indicator showing success or failure of the decryption effort, it is possible for the attacker to use this as an oracle to obtain key equivalent functionality for the CEK used for the chosen recipient of the message. In another use case, an attacker can reduce the tag length of the chosen AEAD cipher for a given AuthEnvelopedData container to be a single byte long, allowing an attacker to brute force CMS decryption, producing an integrity bypass for applications that trust CMS_decrypt() to reject modified content. The FIPS modules are not affected by this issue.	N/A	More Details
CVE-2026-36229	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-0419	Insufficient input validation in NETGEAR JR6150 (AC750 WiFi Router 802.11ac Dual Band Gigabit released in 2014) allows users connected to the local WiFi Networks to execute operating system commands. NETGEAR JR6150 has reached End-of-Support phase as of 2018 , and no further security updates are planned. NETGEAR strongly recommends replacing these devices with newer NETGEAR models to ensure continued security support and updates. This vulnerability has been identified through firmware emulation in a controlled research environment and has not been verified on production hardware.	N/A	More Details
CVE-2026-46486	MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices in order to find signs of a potential compromise. Prior to version 2026.5.12, there is a path traversal vulnerability via unsanitized File identifiers in iOS Backup processing. This issue has been patched in version 2026.5.12.	N/A	More Details
CVE-2026-0418	Insufficient configuration management in the listed devices allows authenticated administrators connected to the local network to tamper with the system.	N/A	More Details
CVE-2026-46314	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Reject empty multisync extension to prevent infinite loop v3d_get_extensions() walks a userspace-provided singly-linked list of ioctl extensions without any bound on the chain length. A local user can craft a self-referential extension (ext->next == &ext) with zero in_sync_count and out_sync_count, which bypasses the existing duplicate-extension guard: if (se->in_sync_count || se->out_sync_count) return -EINVAL; The guard never fires because v3d_get_multisync_post_deps() returns immediately when count is zero, leaving both fields at zero on every iteration. The result is an infinite loop in kernel context, blocking the calling thread and pegging a CPU core indefinitely. Fix this by rejecting a multisync extension where both in_sync_count and out_sync_count are zero in v3d_get_multisync_submit_deps(). An empty multisync carries no synchronization information and serves no useful purpose, so returning -EINVAL for such an extension is the correct defense against this attack vector.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: pmdomain: mediatek: fix use-after-free in scpsys_get_bus_protection_legacy() In scpsys_get_bus_protection_legacy(), of_find_node_with_property() returns a device node with its reference count incremented. The function		

2026-46308	then calls of_node_put(node) before checking whether syscon_regmap_lookup_by_phandle() returns an error. If an error occurs, dev_err_probe() dereferences the node pointer to print diagnostic information, but the node memory may have already been freed due to the earlier of_node_put(), leading to a use-after-free vulnerability. Fix this by moving the of_node_put() call after the error check, ensuring the node is still valid when accessed in the error path.	N/A	More Details
CVE-2026-46309	In the Linux kernel, the following vulnerability has been resolved: drm/xe/uapi: Reject coh_none PAT index for CPU cached memory in madvise Add validation in xe_vm_madvise_ioctl() to reject PAT indices with XE_COH_NONE coherency mode when applied to CPU cached memory. Using coh_none with CPU cached buffers is a security issue. When the kernel clears pages before reallocation, the clear operation stays in CPU cache (dirty). GPU with coh_none can bypass CPU caches and read stale sensitive data directly from DRAM, potentially leaking data from previously freed pages of other processes. This aligns with the existing validation in vm_bind path (xe_vm_bind_ioctl_validate_bo). v2(Matthew brost) - Add fixes - Move one debug print to better place v3(Matthew Auld) - Should be drm/xe/uapi - More Cc v4(Shuicheng Lin) - Fix kmem leak issues by the way v5 - Remove kmem leak because it has been merged by another patch v6 - Remove the fix which is not related to current fix v7 - No change v8 - Rebase v9 - Limit the restrictions to iGPU v10 - No change (cherry picked from commit 016ccdb674b8c899940b3944952c96a6a490d10a)	N/A	More Details
CVE-2026-46310	In the Linux kernel, the following vulnerability has been resolved: media: renesas: vsp1: Fix NULL pointer deref on module unload When unloading the module on gen 4, we hit a NULL pointer dereference. This is caused by the cleanup code calling vsp1_drm_cleanup() where it should be calling vsp1_vspx_cleanup(). Fix this by checking the IP version and calling the drm or vspx function accordingly, the same way as the init code does.	N/A	More Details
CVE-2026-46311	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: fix access to stale wptr mapping Use drm_exec to take both locks i.e vm root bo and wptr_obj bo to access the mapping data properly. This fixes the security issue of unmap the wptr_obj while a queue creation is in progress and passing other bo at same address. (cherry picked from commit 1fc6c8ab45dbee096469c08c13f6099d57a52d6c)	N/A	More Details
CVE-2026-46312	In the Linux kernel, the following vulnerability has been resolved: media: videobuf2: Set vma_flags in vb2_dma_sg_mmap vb2_dma_contig sets VMA flags VM_DONTEXPAND and VM_DONTDUMP and I do not see a reason why vb2_dma_sg should behave differently. This avoids hitting `WARN_ON(!(vma->vm_flags & VM_DONTEXPAND));` in drm_gem_mmap_obj() during mmap() of an imported dma-buf from the out of tree Apple ISP camera capture driver which uses vb2_dma_sg_memops. gst-launch-1.0 v4l2src ! gtk4paintablesink [38.201528] ------------[cut here]------------ [38.202135] WARNING: CPU: 7 PID: 2362 at drivers/gpu/drm/drm_gem.c:1144 drm_gem_mmap_obj+0x1f8/0x210 [38.203278] Modules linked in: rfcomm snd_seq_dummy snd_hrtimer snd_seq snd_seq_device uinput nf_conntrack_netbios_ns nf_conntrack_broadcast nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_inet nf_reject_ipv6 nft_reject nft_ct nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 nf_tables qrtr bnep nls_ascii i2c_dev loop fuse dm_multipath nfnetlink brcmfmac_wcc hid_magicmouse hci_bcm4377 brcmfmac brcmutil bluetooth ecdh_generic cfg80211 ecc btrfs xor xor_neon rfkill hid_apple raid6_pq joydev aop_als apple_nvmem_spmi industrialio snd_soc_aop apple_z2 snd_soc_cs42l84 tps6598x snd_soc_tas2764 macsmc_reboot spi_nor macsmc_hwmon rtc_macsmc gpio_macsmc macsmc_power regmap_spmi macsmc_input dockchannel_hid panel_summit appledrm nvme_apple dwc3 snd_soc_macaudio drm_client_lib nvme_core phy_apple_atc hwmon apple_sart apple_dockchannel macsmc apple_rtkit_helper spmi_apple_controller aop apple_wdt mfd_core nvmem_apple_efuses pinctrl_apple_gpio apple_isp apple_dcp videobuf2_dma_sg mux_core spi_apple [38.203300] videobuf2_memops i2c_pasemi_platform snd_soc_apple_mca videobuf2_v4l2 videodev clk_apple_nco videobuf2_common snd_pcm_dmaengine adpdrm asahi apple_admac adpdrm_mipi drm_dma_helper pwm_apple i2c_pasemi_core drm_display_helper mc cec apple_dart ofpart apple_soc_cpufreq leds_pwm phram [38.217677] CPU: 7 UID: 1000 PID: 2362 Comm: gst-launch-1.0 Tainted: G W 6.17.6+ #asahi-dev PREEMPT(full) [38.219040] Tainted: [W]=WARN [38.219398] Hardware name: Apple MacBook Pro (13-inch, M2, 2022) (DT) [38.220213] pstate: 21400005 (nzCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) [38.221088] pc : drm_gem_mmap_obj+0x1f8/0x210 [38.221643] lr : drm_gem_mmap_obj+0x78/0x210 [38.222178] sp : ffffc0008dc678e0 [38.222579] x29: ffffc0008dc678e0 x28: 0000000000042a97 x27: ffff8000b701b480 [38.223465] x26: 00000000000000fb x25: ffffc0008dc67d20 x24: ffffc0008dc67968 [38.224402] x23: ffff8000e3ca5600 x22: ffff8000265b7800 x21: ffff80003000c0c0 [38.225279] x20: 0000000000000000 x19: ffff8000b68c5200 x18: ffffc0008dc67968 [38.226151] x17: 0000000000000000 x16: 0000000000000000 x15: ffffc000810a30a8 [38.227042] x14: 00007fff637effff x13: 00005555de91ffff x12: 00007fff63293fff [38.227942] x11: 0000000000000000 x10: ffff8000184ecf08 x9 : ffffc0007a1900c8 [38.228824] x8 : ffffc0008dc67968 x7 : 0000000000000012 x6 : ffffc0015cf1c000 [38.229703] x5 : ffffc0008dc676a0 x4 : ffffc00081a27dc0 x3 : 0000000000000038 [38.230607] x2 : 0000000000000003 x1 : 0000000000000003 x0 : 00000000100000fb [38.231488] Call trace: [38.231806] drm_gem_mmap_obj+0x1f8/0x210 (P) [38.232342] drm_gem_mmap+0x140/0x260 [38.232813] __mmap_region+0x488/0x9a0 [38.233277] mmap_region+0xd0/0x148 [38.233703] do_mmap+0x350/0x5c0 [38.234148] vm_mmap_pgoff+0x14c/0x200 [38.234612] ksys_mmap_pgoff+0x150/0x208 [38.235107] __arm64_sys_mmap+0x34/0x50 [38.235611]	N/A	More Details

	invoke_syscall+0x50/0x120 [38.236075] el0_svc_common.constprop.0+0x48/0xf0 [38.236680] do_el0_svc+0x24/0x38 [38.237113] el0_svc+0x38/0x168 [38.237507] el0t_64_sync_handler+0xa0/0xe8 [38.238034] el0t_64_sync+0x198/0x1a0 [38.238491] ---[end trace 0000000000000000]--- There were discussions in [1] at the end of 2023 that mmap() on imported ---truncated---		
CVE-2026-46313	In the Linux kernel, the following vulnerability has been resolved: media: intel/ipu6: fix error pointer dereference In a error path isp->psys is confirmed to be an error pointer not NULL so this condition is true and the error pointer is dereferenced. So isp-psys should be set to NULL before going to out_ipu6_bus_del_devices. Detected by Smatch: drivers/media/pci/intel/ipu6/ipu6.c:690 ipu6_pci_probe() error: 'isp->psys' dereferencing possible ERR_PTR() [Sakari Ailus: Fix commit message.]	N/A	More Details
CVE-2026-0411	An information disclosure vulnerability in the NETGEAR Orbi satellites could allow a user connected to your network to gain administrator access to the Orbi router. The listed NETGEAR models are affected by this vulnerability. Orbi WiFi Systems without satellite devices are not impacted by this issue.	N/A	More Details
CVE-2026-0417	Insufficient input validation vulnerability in NETGEAR devices allows authenticated administrators connected to the local network to tamper with the router's integrity.	N/A	More Details
CVE-2026-0412	Insufficient input validation vulnerability in NETGEAR JR6150 (AC750 WiFi Router 802.11ac Dual Band Gigabit released in 2014) allows administrators connected to the local network to make unauthorized modification of router software and functionality. NETGEAR JR6150 reached End-of-Support status in 2018 and is no longer receiving security updates. NETGEAR strongly recommends replacing these devices with newer NETGEAR models to ensure continued security support and updates. This vulnerability has been identified through firmware emulation in a controlled research environment and has not been verified on production hardware.	N/A	More Details
CVE-2026-0413	Insufficient input validation of buffers vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	N/A	More Details
CVE-2026-0414	Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	N/A	More Details
CVE-2026-0415	Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	N/A	More Details
CVE-2026-0416	Authenticated administrators connected to the local network can modify router functionality beyond what is intended through the standard management interface.	N/A	More Details
CVE-2026-8913	A command Injection vulnerability exists in the WireGuard client configuration of Archer MR600 v5 due to improper neutralization of user-controlled input within the web management interface. An authenticated attacker with administrative privileges may be able to execute arbitrary commands when applying configuration changes.Successful exploitation may result in a full compromise of confidentiality, integrity, and availability of the affected device.	N/A	More Details
CVE-2026-34183	Issue summary: Remote peer may exhaust heap memory of the QUIC server or client by flooding it with packets containing PATH_CHALLENGE frames. Impact summary: A malicious remote peer can cause an unbounded memory allocation which can lead to an abnormal termination of the application acting as a QUIC client or server and a Denial of Service. A remote peer may exhaust heap memory by flooding the local QUIC stack with PATH_CHALLENGE frames. The local QUIC stack allocates a PATH_RESPONSE frame for every PATH_CHALLENGE it receives. The allocated PATH_RESPONSE frame gets freed only when the remote peer acknowledges reception of the PATH_RESPONSE frame which will not be done by a malicious peer. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue. The QUIC stack is outside of OpenSSL FIPS module boundary.	N/A	More Details
CVE-2026-35188	Issue summary: A malicious server can exploit TLS OCSP stapling by delivering a crafted response through the status_request extension, triggering a double-free in the client's certificate verification path. Impact summary: Successful exploitation allows an attacker to corrupt heap memory via a double-free, potentially leading to a Denial of Service or possibly an attacker controlled code execution or other undefined behavior. If OCSP stapling is enabled and the TLS client connects to a malicious server, a crafted OCSP stapled response can trigger a double free in the TLS client when the stapled response is checked. The OCSP stapling is not enabled by default. Reliable code execution through a double-free is technically complex and highly environment-dependent but the Denial of Service impact is straightforward to achieve, warranting Moderate severity. No FIPS modules are affected by this issue as the affected code is outside the OpenSSL FIPS module boundary.	N/A	More Details

CVE-2026-46318	In the Linux kernel, the following vulnerability has been resolved: Revert "mm/hugetlbfs: update hugetlbfs to use mmap_prepare" This reverts commit ea52cb24cd3f ("mm/hugetlbfs: update hugetlbfs to use mmap_prepare") with conflict resolution to account for changes in commit ea52cb24cd3f ("mm/hugetlbfs: update hugetlbfs to use mmap_prepare"). The patch incorrectly handled hugetlb VMA lock allocation at the mmap_prepare stage, where a failed allocation occurring after mmap_prepare is called might result in the lock leaking. There is no risk of a merge causing a similar issues, as VMA_DONTEXPAND_BIT is set for hugetlb mappings. As a first step in addressing this issue, simply revert the change so we can rework how we do this having corrected the underlying issues. We maintain the VMA flags changes as best we can, accounting for the fact that we were working with a VMA descriptor previously and propagating like-for-like changes for this. Note that we invoke vma_set_flags() and do not call vma_start_write() as vm_flags_set() does. This is OK as it's being done in an .mmap hook where the VMA is not yet linked into the tree so nobody else can be accessing it.	N/A	More Details
CVE-2026-38615	DedeCMS V5.7.118 is vulnerable to Command Execution in file_manage_control.php.	N/A	More Details
CVE-2026-11429	Two endpoints in the Vault Service ScriptsController, shared by Altium Enterprise Server and Altium 365, accept file uploads where a user-supplied filename component is used to construct the destination path without validation, allowing arbitrary files to be written to any location writable by the service account. Because the file write operation completes before authentication is validated, the vulnerability can be exploited without any credentials, session, or prior knowledge of the system. An unauthenticated network attacker can use this primitive to place executable content in directories where it is later executed by the service, resulting in remote code execution under the Vault Service account. Altium Enterprise Server is fixed in 8.1.1; the issue has been remediated in Altium 365 (commercial and government cloud) at the service level.	N/A	More Details
CVE-2026-41065	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 are vulnerable to remote code execution via the newsletter custom template directory feature. On a fresh install before the setup wizard is completed, all management endpoints are completely unauthenticated. An attacker can create a newsletter agent, point the custom template directory to an attacker-controlled SMB share serving a malicious Mako template, and trigger execution via the newsletter render endpoint, all with zero credentials and no local access to the target system. On a completed install with credentials configured, the same chain is exploitable by any admin. Version 2.17.1 fixes the issue.	N/A	More Details
CVE-2026-11431	A path traversal vulnerability exists in the Projects Service download endpoint shared by Altium Enterprise Server and Altium 365. An authenticated user can supply a crafted path parameter that bypasses validation, allowing arbitrary files (including entire directories returned as archives) to be read from the server filesystem. Because the readable files include service configuration and credential material, exploitation can be used to gather information enabling further compromise. The issue can be combined with CVE-2026-11424 to reach the cloud-side endpoint. On multi-tenant Altium 365 deployments, the readable configuration could have exposed credentials shared across services. Altium Enterprise Server is fixed in 8.1.1; the issue has been remediated in Altium 365 at the service level.	N/A	More Details
CVE-2026-45409	Internationalized Domain Names in Applications (IDNA) for Python provides support for Internationalized Domain Names in Applications (IDNA) and Unicode IDNA Compatibility Processing. In versions prior to 3.15, payloads such as `"\u0660" * N` or `"\u30fb" * N + "\u6f22"` utilize the `valid_contexto` function prior to length rejection, and for high values of `N` will take a long time to process. This is the same issue as CVE-2024-3651, however the original remediation in 2024 was not a complete fix. A specially crafted argument to the `idna.encode()` function could consume significant resources. This may lead to a denial-of-service. Starting in version 3.14, the function rejects long inputs as soon as practicable prior to any further processing to minimize resource consumption. In version 3.15, this approach was extended to lesser used alternate functions (i.e. per-label conversions and codec support). A workaround is available. Domain names cannot exceed 253 characters in length. If this length limit is enforced prior to passing the domain to the `idna.encode()` function, it should no longer consume significant resources. This is triggered by arbitrarily large inputs that would not occur in normal usage, but may be passed to the library assuming there is no preliminary input validation by the higher-level application.	N/A	More Details
CVE-2026-34123	On Tapo C520WS v2, restricted accounts (for example, hub users) are intended to execute only a limited set of low-sensitivity operations. Due to a logic flaw in the device’s API authorization mechanism, an attacker can craft requests that leverage legitimate “method mapping” behavior to bypass whitelist restrictions, allowing restricted operations to be masked as permitted requests and executed. Successful exploitation may allow an attacker (with access to a restricted account) to execute unauthorized sensitive operations. Depending on the operation invoked, impact could include device resets, unintended configuration changes, or disruption of normal operation, leading to loss of availability and integrity of the device.	N/A	More Details
CVE-	A stack-based buffer overflow vulnerability exists in Tapo C520WS v2 in the ONVIF CreateUsers service, where the device fails to properly validate the number of XML user nodes during request processing. An		

2026-6239	authenticated attacker can send a specially crafted ONVIF request containing an excessive number of user entries to trigger memory corruption. Successful exploitation may cause the ONVIF management service to terminate unexpectedly, resulting in a denial-of-service (DoS) condition that disrupts device configuration and management functions.	N/A	More Details
CVE-2026-6240	A stack-based buffer overflow vulnerability exists in Tapo C520WS v2 in the ONVIF DeleteUsers service, due to insufficient boundary checks when handling multiple user deletion parameters. An authenticated attacker can send a crafted malicious request containing an excessive number of identifiers to overflow stack memory. Successful exploitation may result in a service crash or deadlock, leading to DoS affecting device management and monitoring functionality.	N/A	More Details
CVE-2026-6241	An authenticated format string vulnerability is present in the ONVIF AddScopes in Tapo C520WS v2, where user-controlled input is improperly passed to formatting functions without adequate sanitization. An attacker can inject format specifiers into ONVIF scope parameters to manipulate memory handling behavior. Successful exploitation may cause the ONVIF management service to crash, resulting in DoS condition that impacts normal device operation.	N/A	More Details
CVE-2026-11029	Insufficient validation of untrusted input in Drag and Drop in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2026-6242	An authenticated format string vulnerability exists in the ONVIF Subscribe service in Tapo C520WS v2 due to improper handling of externally supplied parameters within formatting functions. An attacker may inject crafted format strings into event subscription requests or notification generation path to disrupt normal service execution. Successful exploitation may cause the event notification service to terminate unexpectedly, resulting in the loss of real-time alarm functionality and disruption of event notifications.	N/A	More Details
CVE-2026-41522	Iris is a web collaborative platform that helps incident responders share technical details during investigations. Prior to version 2.4.28, DFIR-IRIS exposes an optional GraphQL endpoint at `/graphql` that does not enforce the same authorization checks as the REST API. Any authenticated user can abuse it in three ways: unauthorized IOC read across cases (IDOR), bulk IOC disclosure via `case.iocs`. The `case(caseId: ...).iocs` resolver returns IOCs linked to an arbitrary case without verifying the caller has access to that case, and unauthorized case creation. All three are reachable by any authenticated user, regardless of role or case ACL. This is fixed in v2.4.28. The GraphQL blueprint, resolvers, and dependencies (`graphene`, `graphene-sqlalchemy`, `graphql-server[flask]`) were removed entirely, since the feature was not in use. As a workaround, block `/graphql` at the reverse proxy (recommended) or comment out the `graphql_blueprint` import and `register_blueprint` call in `source/app/views.py` and restart.	N/A	More Details
CVE-2026-10868	A mass assignment vulnerability exists in the MISP user edit functionality due to insufficient filtering of user-supplied fields in UsersController::edit(). When processing edit requests, the application accepted a user-controlled User.id value from request data. An authenticated attacker could craft a modified request containing another user identifier, potentially causing updates to be applied to an unintended user account. Depending on the editable fields and the attacker's privileges, this could allow unauthorized modification of user account attributes and impact account integrity. The issue was addressed by explicitly removing the User.id field from request data before processing the user edit operation.	N/A	More Details
CVE-2026-48480	The netty incubator codec.bhttp is a java language binary http parser. Prior to version 0.0.22.FInal, the codec-ohttp implementation of draft-ietf-ohai-chunked-ohttp does not verify that a cryptographically-signed final chunk was received before the outer HTTP body terminates. An on-path adversary (the OHTTP relay itself, or any MITM on the relay↔gateway or relay↔client transport) can forward a prefix of a legitimate chunked-OHTTP message—cut at a non-final chunk boundary—and close the outer body cleanly, producing no decryption error and no exception in the receiving application. Version 0.0.22.Final fixes the issue.	N/A	More Details
CVE-2026-41237	Froxlor is open source server administration software. In version 2.3.6 and earlier, the LOC record regex uses `\s+` which matches newlines (allowing embedded newlines to pass), TLSA `matchingType=0` has no upper bound on hex data length, and all validators return raw input without zone-file escaping. Version 2.3.7 contains an updated patch.	N/A	More Details
CVE-2026-41235	Froxlor is open source server administration software. Version 2.3.6 lets administrators configure `system.available_shells` as the approved shell list that customers may assign to FTP users. However, the server-side FTP account handlers do not enforce that whitelist when processing add or edit requests. As a result, an authenticated customer with shell delegation enabled can submit an arbitrary shell such as `/bin/bash` even when the panel UI only offers more restricted choices. In deployments that use the default `nssextrausers` integration, the attacker-controlled shell is then propagated into the system account database, leading to real host shell access. Version 2.3.7 fixes the issue.	N/A	More Details
	A server-side request forgery (SSRF) vulnerability exists in a GraphQL service component shared by Altium Enterprise Server and Altium 365. An authenticated user can submit a request whose input is		

CVE-2026-11424	treated as a URL by the server and used to issue an outbound HTTP GET request without URL validation or destination filtering. The response body is then returned to the user. This allows an authenticated attacker to reach internal services and metadata endpoints that would not otherwise be accessible from the public network, and to retrieve their contents. The impact is information disclosure and internal infrastructure reconnaissance; the request primitive is limited to HTTP GET with no custom headers. Altium Enterprise Server is fixed in 8.1.1; the issue has been remediated in Altium 365 at the service level.	N/A	More Details
CVE-2026-11423	A path traversal vulnerability exists in the Altium Enterprise Server Collaboration Service due to improper handling of user-supplied filenames in the MCAD and Simulation file download flows. A regular authenticated user can submit a collaboration message containing a crafted filename, which is later used to construct the download path on the server without validation, allowing arbitrary files to be read from the server filesystem. Because the readable files include the server's master configuration, which stores credentials for privileged accounts, exploitation can lead to authenticating as a system administrator and gaining full control of the server. Altium 365 cloud deployments are not affected.	N/A	More Details
CVE-2026-46401	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Versions prior to 26.0.0 suffer from an improper session termination vulnerability where authentication tokens remain valid after user logout. This allows attackers who obtain valid tokens to maintain persistent access to authenticated CMS functionality, bypassing the intended session termination mechanism and enabling unauthorized access to CMS metadata and administrative functions. Version 26.0.0 fixes the issue.	N/A	More Details
CVE-2026-45777	OpenXDMoD is an open framework for collecting and analyzing HPC metrics. Starting in version 9.5.0 and prior to version 11.0.3, an attacker can remotely execute arbitrary system commands on the web server hosting Open XDMoD with the privileges of the web server process. This could allow an attacker to read or modify application data, alter system configuration, or disrupt service availability. All deployments of Open XDMoD versions 9.5.0 through 11.0.2 (inclusive) are impacted. This issue was reported privately on 2026-04-06, and at this time there is no evidence that this vulnerability has been exploited in the wild. The vulnerability was patched in Open XDMoD 11.0.3 on 2026-05-12. As a workaround, apply the patch manually.	N/A	More Details
CVE-2026-3088	Unauthenticated users on the local network can cause the router to become unavailable by sending specially crafted requests.	N/A	More Details
CVE-2026-11326	OpenAI Atlas before 1.2025.288.15 exposed privileged browser APIs to web content on *.openai.com origins. A cross-site scripting vulnerability in forum.openai.com could be used to access these functions, allowing access to browser history information and the ability to open or close tabs. OpenAI Atlas 1.2025.288.15 narrows access to these APIs to *.chatgpt.com; users should upgrade to 1.2025.288.15 or later.	N/A	More Details
CVE-2026-42567	Svelte is a performance oriented web framework. From version 5.51.5 to before version 5.55.7, an internal regex in the Svelte runtime can take exponential time to test in <svelte:element this={tag}> </svelte:element>. This issue has been patched in version 5.55.7.	N/A	More Details
CVE-2026-42573	Svelte is a performance oriented web framework. Prior to version 5.55.7, Svelte was vulnerable to DOM clobbering of its internal framework state on elements, potentially leading to XSS attacks. This issue has been patched in version 5.55.7.	N/A	More Details
CVE-2026-42599	Svelte is a performance oriented web framework. Prior to version 5.55.7, when using spread syntax to render attributes from untrusted data, event handler properties are included in the rendered HTML output. If an application spreads user-controlled or external data as element attributes, an attacker can inject malicious event handlers that execute in victims' browsers. Note that this vulnerability only triggers if the user's browser has JavaScript enabled but Svelte's hydration mechanism does not reach the vulnerable element before the event fires. This issue has been patched in version 5.55.7.	N/A	More Details
CVE-2026-45776	OpenXDMoD is an open framework for collecting and analyzing HPC metrics. Prior to version 11.0.3, a flaw in Open XDMoD's access control logic allows an attacker to submit a crafted HTTPS POST request that sets a session variable used for authorization decisions. If an installation of Open XDMoD includes the optional Job Performance (SUPReMM) module, an attacker could bypass intended data access restrictions and view other users' compute job efficiency metrics. All deployments of Open XDMoD prior to version 11.0.3 that contain the optional Job Performance (SUPReMM) module are impacted. This issue was reported privately on 2026-04-06, and at this time there is no evidence that this vulnerability has been exploited in the wild. The vulnerability was patched in Open XDMoD 11.0.3 on 2026-05-12. As a workaround, apply the patch manually.	N/A	More Details
CVE-2026-	OpenXDMoD is an open framework for collecting and analyzing HPC metrics. Prior to version 11.0.3, an authenticated attacker can inject malicious JavaScript into their Open XDMoD user profile and abuse the password reset functionality to email a link to an HTML page, which when visited by the victim, reflects and executes the unsanitized payload in the victim's browser, potentially leading to credential capture	N/A	More

45778	and Open XDMoD account takeover. All deployments of Open XDMoD prior to 11.0.3 are impacted. This issue was reported privately on 2026-04-06, and at this time there is no evidence that this vulnerability has been exploited in the wild. The vulnerability was patched in Open XDMoD 11.0.3 on 2026-05-12. As a workaround, apply the patch manually.		Details
CVE-2026-46400	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Starting in version 11.0.6 and prior to version 25.0.0, the file upload functionality in HAXCMS PHP only validates file extensions using a regex pattern without checking the actual file content or MIME type. This allows attackers to upload malicious files (e.g., PHP webshells) disguised as legitimate image files, potentially leading to remote code execution. Version 25.0.0 contains a fix for the issue.	N/A	More Details
CVE-2026-45779	OpenXDMoD is an open framework for collecting and analyzing HPC metrics. An SQL injection vulnerability exists in Open XDMoD versions prior to 10.0.3 that allows an unauthenticated remote attacker to execute arbitrary SQL statements. Exploitation requires no authentication or user interaction and can result in complete compromise of the underlying database. All deployments of Open XDMoD prior to 10.0.3 are impacted. This issue was discovered on 2023-08-03 and patched on 2023-08-04. At this time there is no evidence that this vulnerability has been exploited in the wild. The vulnerability was patched in Open XDMoD 10.0.3 on 2023-08-04. As a workaround, apply the patch manually.	N/A	More Details
CVE-2026-40605	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.1, a path traversal vulnerability in the cache deletion endpoint allows authenticated API access to delete directories outside the configured cache path. This can cause arbitrary data loss and service disruption. Version 2.17.1 fixes the issue.	N/A	More Details
CVE-2026-43926	FOSSBilling is a free, open-source billing and client management system. Prior to version 0.8.0, the password reset confirmation endpoint `/client/reset-password-confirm/:hash` is handled by a non-API controller and is not covered by FOSSBilling's rate limiter, which only applies to `/api/*` routes. This allows an attacker to probe the endpoint for valid reset tokens without any per-IP request limiting, attempt counting, or lockout mechanism. The endpoint acts as an oracle, returning a distinguishable response for valid versus invalid tokens (HTTP 200 vs HTTP 302 redirect). An attacker can submit unlimited token guesses to the password reset confirmation endpoint with no throttling applied. However, practical exploitability is significantly mitigated by the current token generation, which uses `hash('sha256', random_bytes(32))`, providing 256 bits of entropy. Tokens also expire after 15 minutes and are deleted after successful use. The same architectural gap applies to other controller-served auth routes, including `/staff/email/:hash` (admin password reset confirmation) and `/client/confirm-email/:hash` (email confirmation). Version 0.8.0 fixes the issue. Some workarounds are available. Configure a reverse proxy (e.g., Nginx, Apache, Cloudflare) to apply per-IP rate limiting to the `/client/reset-password-confirm/*` and `/staff/email/*` paths and/or use a WAF rule to limit request rates to these endpoints.	N/A	More Details
CVE-2026-45433	This vulnerability exists in GX Earth 2022 ONT models due to the presence of hardcoded RSA private key within the device firmware. A remote attacker could exploit this vulnerability by extracting the cryptographic private key from the firmware, which could lead to decryption of HTTPS traffic and Man-in-the-Middle (MITM) attacks on the targeted device.	N/A	More Details
CVE-2026-8762	Rejected reason: After analysis, the originally reported behaviour was determined not to constitute a security vulnerability. The findings were parser-strictness defects without an exploitable framing-disagreement path in any tested deployment configuration.	N/A	More Details
CVE-2026-46398	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Starting in version 25.0.0 and prior to version 26.0.0, the haxcms_refresh_token cookie is set without the Secure flag. This allows it to be transmitted over unencrypted HTTP, making it vulnerable to theft via packet sniffing on the network. Version 26.0.0 fixes the issue.	N/A	More Details
CVE-2026-46307	In the Linux kernel, the following vulnerability has been resolved: wifi: ath5k: do not access array OOB Vincent reports: > The ath5k driver seems to do an array-index-out-of-bounds access as > shown by the UBSAN kernel message: > UBSAN: array-index-out-of-bounds in drivers/net/wireless/ath/ath5k/base.c:1741:20 > index 4 is out of range for type 'ieee80211_tx_rate [4]' > ... > Call Trace: > <TASK> > dump_stack_lvl+0x5d/0x80 > ubsan_epilogue+0x5/0x2b > __ubsan_handle_out_of_bounds.cold+0x46/0x4b > ath5k_tasklet_tx+0x4e0/0x560 [ath5k] > tasklet_action_common+0xb5/0x1c0 It is real. 'ts->ts_final_idx' can be 3 on 5212, so: info->status.rates[ts->ts_final_idx + 1].idx = -1; with the array defined as: struct ieee80211_tx_rate rates[IEEE80211_TX_MAX_RATES]; while the size is: #define IEEE80211_TX_MAX_RATES 4 is indeed bogus. Set this 'idx = -1' sentinel only if the array index is less than the array size. As mac80211 will not look at rates beyond the size (IEEE80211_TX_MAX_RATES). Note: The effect of the OOB write is negligible. It just overwrites the next member of info->status, i.e. ack_signal.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: flow_dissector: do not dissect PPPoE PFC frames RFC 2516 Section 7 states that Protocol Field Compression (PFC) is NOT RECOMMENDED for PPPoE. In practice, pppd does not support negotiating PFC for PPPoE sessions, and the flow dissector		

CVE-2026-46306	driver has assumed an uncompressed frame until the blamed commit. During the review process of that commit [1], support for PFC is suggested. However, having a compressed (1-byte) protocol field means the subsequent PPP payload is shifted by one byte, causing 4-byte misalignment for the network header and an unaligned access exception on some architectures. The exception can be reproduced by sending a PPPoE PFC frame to an ethernet interface of a MIPS board, with RPS enabled, even if no PPPoE session is active on that interface: $ 0 : 00000000 80c40000 00000000 85144817 $ 4 : 00000008 00000100 80a75758 81dc9bb8 $ 8 : 00000010 8087ae2c 0000003d 00000000 $12 : 000000e0 00000039 00000000 00000000 $16 : 85043240 80a75758 81dc9bb8 00006488 $20 : 0000002f 00000007 85144810 80a70000 $24 : 81d1bda0 00000000 $28 : 81dc8000 81dc9aa8 00000000 805ead08 Hi : 00009d51 Lo : 2163358a epc : 805e91f0 __skb_flow_dissect+0x1b0/0x1b50 ra : 805ead08 __skb_get_hash_net+0x74/0x12c Status: 11000403 KERNEL EXL IE Cause : 40800010 (ExcCode 04) BadVA : 85144817 PrId : 0001992f (MIPS 1004Kc) Call Trace: [<805e91f0>] __skb_flow_dissect+0x1b0/0x1b50 [<805ead08>] __skb_get_hash_net+0x74/0x12c [<805ef330>] get_rps_cpu+0x1b8/0x3fc [<805fca70>] netif_receive_skb_list_internal+0x324/0x364 [<805fd120>] napi_complete_done+0x68/0x2a4 [<8058de5c>] mtk_napi_rx+0x228/0xfec [<805fd398>] __napi_poll+0x3c/0x1c4 [<805fd754>] napi_threaded_poll_loop+0x234/0x29c [<805fd848>] napi_threaded_poll+0x8c/0xb0 [<80053544>] kthread+0x104/0x12c [<80002bd8>] ret_from_kernel_thread+0x14/0x1c Code: 02d51821 1060045b 00000000 <8c640000> 3084000f 2c820005 144001a2 00042080 8e220000 To reduce the attack surface and maintain performance, do not process PPPoE PFC frames. [1] https://lore.kernel.org/r/20220630231016.GA392@debian.home	N/A	More Details
CVE-2026-46305	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: os_dep: avoid NULL pointer dereference in rtw_cbuf_alloc The return value of kzalloc_flex() is used without ensuring that the allocation succeeded, and the pointer is dereferenced unconditionally. Guard the access to the allocated structure to avoid a potential NULL pointer dereference if the allocation fails.	N/A	More Details
CVE-2026-46304	In the Linux kernel, the following vulnerability has been resolved: nvmet: avoid recursive nvmet-wq flush in nvmet_ctrl_free nvmet_tcp_release_queue_work() runs on nvmet-wq and can drop the final controller reference through nvmet_cq_put(). If that triggers nvmet_ctrl_free(), the teardown path flushes ctrl->async_event_work on the same nvmet-wq. Call chain: nvmet_tcp_schedule_release_queue() kref_put(&queue->kref, nvmet_tcp_release_queue) nvmet_tcp_release_queue() queue_work(nvmet_wq, &queue->release_work) <--- nvmet_wq process_one_work() nvmet_tcp_release_queue_work() nvmet_cq_put(&queue->nvme_cq) nvmet_cq_destroy() nvmet_ctrl_put(cq->ctrl) nvmet_ctrl_free() flush_work(&ctrl->async_event_work) <--- nvmet_wq Previously Scheduled by :- nvmet_add_async_event queue_work(nvmet_wq, &ctrl->async_event_work); This trips lockdep with a possible recursive locking warning. [5223.015876] run blktests nvme/003 at 2026-04-07 20:53:55 [5223.061801] loop0: detected capacity change from 0 to 2097152 [5223.072206] nvmet: adding nsid 1 to subsystem blktests-subsystem-1 [5223.088368] nvmet_tcp: enabling port 0 (127.0.0.1:4420) [5223.126086] nvmet: Created discovery controller 1 for subsystem nqn.2014-08.org.nvmexpress.discovery for NQN nqn.2014-08.org.nvmexpress:uuid:0f01fb42-9f7f-4856-b0b3-51e60b8de349. [5223.128453] nvme nvme1: new ctrl: NQN "nqn.2014-08.org.nvmexpress.discovery", addr 127.0.0.1:4420, hostnqn: nqn.2014-08.org.nvmexpress:uuid:0f01fb42-9f7f-4856-b0b3-51e60b8de349 [5233.199447] nvme nvme1: Removing ctrl: NQN "nqn.2014-08.org.nvmexpress.discovery" [5233.227718] == [5233.231283] WARNING: possible recursive locking detected [5233.234696] 7.0.0-rc3nvme+ #20 Tainted: G O N [5233.238434] -- [5233.241852] kworker/u192:6/2413 is trying to acquire lock: [5233.245429] ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: touch_wq_lockdep_map+0x26/0x90 [5233.251438] but task is already holding lock: [5233.255254] ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x5cc/0x6e0 [5233.261125] other info that might help us debug this: [5233.265333] Possible unsafe locking scenario: [5233.269217] CPU0 [5233.270795] ---- [5233.272436] lock((wq_completion)nvmet-wq); [5233.275241] lock((wq_completion)nvmet-wq); [5233.278020] *** DEADLOCK *** [5233.281793] May be due to missing lock nesting notation [5233.286195] 3 locks held by kworker/u192:6/2413: [5233.289192] #0: ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x5cc/0x6e0 [5233.294569] #1: ffffc9000e2a7e40 ((work_completion)(&queue->release_work)){+.+.}-{0:0}, at: process_one_work+0x1c5/0x6e0 [5233.300128] #2: ffffffff82d7dc40 (rcu_read_lock){....}-{1:3}, at: __flush_work+0x62/0x530 [5233.304290] stack backtrace: [5233.306520] CPU: 4 UID: 0 PID: 2413 Comm: kworker/u192:6 Tainted: G O N 7.0.0-rc3nvme+ #20 PREEMPT(full) [5233.306524] Tainted: [O]=OOT_MODULE, [N]=TEST [5233.306525] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 [5233.306527] Workqueue: nvmet-wq nvmet_tcp_release_queue_work [nvmet_tcp] [5233.306532] Call Trace: [5233.306534] <TASK> [5233.306536] dump_stack_lvl+0x73/0xb0 [5233.306552] print_deadlock_bug+0x225/0x2f0 [5233.306556] __lock_acquire+0x13f0/0x2290 [5233.306563] lock_acquire+0xd0/0x300 [5233.306565] ? touch_wq_lockdep_map+0x26/0x90 [5233.306571] ? __flush_work+0x20b/0x530 [5233.306573] ? touch_wq_lockdep_map+0x26/0x90 [5233.306577] touch_wq_lockdep_map+0x3b/0x90 [5233.306580] ? touch_wq_lockdep_map+0x26/0x90 [52 ---truncated---	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Fix segfault when updating ftrace mask Fix invalid data access by passing right data for debugfs entry. [171.549793]		

CVE-2026-46278	Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [171.559248] Mem abort info: [171.562173] ESR = 0x0000000096000044 [171.566227] EC = 0x25: DABT (current EL), IL = 32 bits [171.573108] SET = 0, FnV = 0 [171.576448] EA = 0, S1PTW = 0 [171.579745] FSC = 0x04: level 0 translation fault [171.584760] Data abort info: [171.588012] ISV = 0, ISS = 0x00000044, ISS2 = 0x00000000 [171.593734] CM = 0, WnR = 1, TnD = 0, TagAccess = 0 [171.598962] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [171.604471] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000083837000 [171.611358] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 [171.618500] Internal error: Oops: 0000000096000044 [#1] SMP [171.624222] Modules linked in: powervr drm_shmem_helper drm_gpuvm... [171.656580] CPU: 0 UID: 0 PID: 549 Comm: bash Not tainted 7.0.0-rc2-g730b257ba723-dirty #13 PREEMPT [171.665773] Hardware name: BeagleBoard.org BeaglePlay (DT) [171.671296] pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [171.678306] pc : pvr_fw_trace_mask_set+0x78/0x154 [powervr] [171.683959] lr : pvr_fw_trace_mask_set+0x4c/0x154 [powervr] [171.689593] sp : ffff8000835ebb90 [171.692929] x29: ffff8000835ebc00 x28: ffff000005c60f80 x27: 0000000000000000 [171.700130] x26: 0000000000000000 x25: ffff00000504af28 x24: 0000000000000000 [171.707324] x23: ffff00000504af50 x22: 0000000000000203 x21: 0000000000000000 [171.714518] x20: ffff000005c44a80 x19: ffff000005c457b8 x18: 0000000000000000 [171.721715] x17: 0000000000000000 x16: 0000000000000000 x15: 0000aaaae8887580 [171.728908] x14: 0000000000000000 x13: 0000000000000000 x12: ffff8000835ebc30 [171.736095] x11: ffff00000504af2a x10: ffff00008504af29 x9 : 0fffffffffffffff [171.743286] x8 : ffff8000835ebbf8 x7 : 0000000000000000 x6 : 000000000000002a [171.750479] x5 : ffff00000504af2e x4 : 0000000000000000 x3 : 0000000000000010 [171.757674] x2 : 0000000000000203 x1 : 0000000000000000 x0 : ffff8000835ebba0 [171.764871] Call trace: [171.767342] pvr_fw_trace_mask_set+0x78/0x154 [powervr] (P) [171.772984] simple_attr_write_xsigned.isra.0+0xe0/0x19c [171.778341] simple_attr_write+0x18/0x24 [171.782296] debugfs_attr_write+0x50/0x98 [171.786341] full_proxy_write+0x6c/0xa8 [171.790208] vfs_write+0xd4/0x350 [171.793561] ksys_write+0x70/0x108 [171.796995] __arm64_sys_write+0x1c/0x28 [171.800952] invoke_syscall+0x48/0x10c [171.804740] el0_svc_common.constprop.0+0x40/0xe0 [171.809487] do_el0_svc+0x1c/0x28 [171.812834] el0_svc+0x34/0x108 [171.816013] el0t_64_sync_handler+0xa0/0xe4 [171.820237] el0t_64_sync+0x198/0x19c [171.823939] Code: 32000262 b90ac293 1a931056 9134e293 (b9000036) [171.830073] ---[end trace 0000000000000000]---	N/A	More Details
CVE-2026-46279	In the Linux kernel, the following vulnerability has been resolved: mm/alloc_tag: clear codetag for pages allocated before page_ext initialization Due to initialization ordering, page_ext is allocated and initialized relatively late during boot. Some pages have already been allocated and freed before page_ext becomes available, leaving their codetag uninitialized. A clear example is in init_section_page_ext(): alloc_page_ext() calls kmemleak_alloc(). If the slab cache has no free objects, it falls back to the buddy allocator to allocate memory. However, at this point page_ext is not yet fully initialized, so these newly allocated pages have no codetag set. These pages may later be reclaimed by KASAN, which causes the warning to trigger when they are freed because their codetag ref is still empty. Use a global array to track pages allocated before page_ext is fully initialized. The array size is fixed at 8192 entries, and will emit a warning if this limit is exceeded. When page_ext initialization completes, set their codetag to empty to avoid warnings when they are freed later. This warning is only observed with CONFIG_MEM_ALLOC_PROFILING_DEBUG=Y and mem_profiling_compressed disabled: [9.582133] ------------[cut here]------------ [9.582137] alloc_tag was not set [9.582139] WARNING: ./include/linux/alloc_tag.h:164 at __pgalloc_tag_sub+0x40f/0x550, CPU#5: systemd/1 [9.582190] CPU: 5 UID: 0 PID: 1 Comm: systemd Not tainted 7.0.0-rc4 #1 PREEMPT(lazy) [9.582192] Hardware name: Red Hat KVM, BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [9.582194] RIP: 0010:__pgalloc_tag_sub+0x40f/0x550 [9.582196] Code: 00 00 4c 29 e5 48 8b 05 1f 88 56 05 48 8d 4c ad 00 48 8d 2c c8 e9 87 fd ff ff 0f 0b 0f 0b e9 f3 fe ff ff 48 8d 3d 61 2f ed 03 <67> 48 0f b9 3a e9 b3 fd ff ff 0f 0b eb e4 e8 5e cd 14 02 4c 89 c7 [9.582197] RSP: 0018:ffffc9000001f940 EFLAGS: 00010246 [9.582200] RAX: dfffffc0000000000 RBX: 1ffff92000003f2b RCX: 1ffff110200d806c [9.582201] RDX: ffff8881006c0360 RSI: 0000000000000004 RDI: ffffffff9bc7b460 [9.582202] RBP: 0000000000000000 R08: 0000000000000000 R09: fffffbfff3a62324 [9.582203] R10: ffffffff9d311923 R11: 0000000000000000 R12: ffffea0004001b00 [9.582204] R13: 0000000000002000 R14: ffffea0000000000 R15: ffff8881006c0360 [9.582206] FS: 00007ffbbcf2d940(0000) GS:ffff888450479000(0000) knlGS:0000000000000000 [9.582208] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [9.582210] CR2: 000055ee3aa260d0 CR3: 0000000148b67005 CR4: 0000000000770ef0 [9.582211] PKRU: 55555554 [9.582212] Call Trace: [9.582213] <TASK> [9.582214] ? __pfx___pgalloc_tag_sub+0x10/0x10 [9.582216] ? check_bytes_and_report+0x68/0x140 [9.582219] __free_frozen_pages+0x2e4/0x1150 [9.582221] ? __free_slab+0xc2/0x2b0 [9.582224] qlist_free_all+0x4c/0xf0 [9.582227] kasan_quarantine_reduce+0x15d/0x180 [9.582229] __kasan_slab_alloc+0x69/0x90 [9.582232] kmem_cache_alloc_noprof+0x14a/0x500 [9.582234] do_getname+0x96/0x310 [9.582237] do_readlinkat+0x91/0x2f0 [9.582239] ? __pfx_do_readlinkat+0x10/0x10 [9.582240] ? get_random_bytes_user+0x1df/0x2c0 [9.582244] __x64_sys_readlinkat+0x96/0x100 [9.582246] do_syscall_64+0xce/0x650 [9.582250] ? __x64_sys_getrandom+0x13a/0x1e0 [9.582252] ? __pfx___x64_sys_getrandom+0x10/0x10 [9.582254] ?	N/A	More Details

	do_syscall_64+0x114/0x650 [9.582255] ? ksys_read+0xfc/0x1d0 [9.582258] ? __pfx_ksys_read+0x10/0x10 [9.582260] ? do_syscall_64+0x114/0x650 [9.582262] ? do_syscall_64+0x114/0x650 [9.582264] ? __pfx_fput_close_sync+0x10/0x10 [9.582266] ? file_close_fd_locked+0x178/0x2a0 [9.582268] ? __x64_sys_faccessat2+0x96/0x100 [9.582269] ? __x64_sys_close+0x7d/0xd0 [9.582271] ? do_syscall_64+0x114/0x650 [9.582273] ? do_syscall_64+0x114/0x650 [9.582275] ? clear_bhb_loop+0x50/0xa0 [9.582277] ? clear_bhb_l ---truncated---		
CVE-2026-46280	In the Linux kernel, the following vulnerability has been resolved: lib: test_hmm: evict device pages on file close to avoid use-after-free Patch series "Minor hmm_test fixes and cleanups". Two bugfixes a cleanup for the HMM kernel selftests. These were mostly reported by Zenghui Yu with special thanks to Lorenzo for analysing and pointing out the problems. This patch (of 3): When dmirror_fops_release() is called it frees the dmirror struct but doesn't migrate device private pages back to system memory first. This leaves those pages with a dangling zone_device_data pointer to the freed dmirror. If a subsequent fault occurs on those pages (eg. during coredump) the dmirror_devmem_fault() callback dereferences the stale pointer causing a kernel panic. This was reported [1] when running mm/ksft_hmm.sh on arm64, where a test failure triggered SIGABRT and the resulting coredump walked the VMAs faulting in the stale device private pages. Fix this by calling dmirror_device_evict_chunk() for each devmem chunk in dmirror_fops_release() to migrate all device private pages back to system memory before freeing the dmirror struct. The function is moved earlier in the file to avoid a forward declaration.	N/A	More Details
CVE-2026-46281	In the Linux kernel, the following vulnerability has been resolved: vmalloc: fix buffer overflow in vrealloc_node_align() Commit 4c5d3365882d ("mm/vmalloc: allow to set node and align in vrealloc") added the ability to force a new allocation if the current pointer is on the wrong NUMA node, or if an alignment constraint is not met, even if the user is shrinking the allocation. On this path (need_realloc), the code allocates a new object of 'size' bytes and then memcpy()s 'old_size' bytes into it. If the request is to shrink the object (size < old_size), this results in an out-of-bounds write on the new buffer. Fix this by bounding the copy length by the new allocation size.	N/A	More Details
CVE-2026-4881	In affected versions of Octopus Server, permissions were not checked correctly resulting in any authenticated user being able to make server level changes using a certain API endpoint despite receiving an error.	N/A	More Details
CVE-2026-46326	In the Linux kernel, the following vulnerability has been resolved: iio: pressure: mprls0025pa: fix spi_transfer struct initialisation Make sure that the spi_transfer struct is zeroed out before use.	N/A	More Details
CVE-2026-46327	In the Linux kernel, the following vulnerability has been resolved: dm: fix unlocked test for dm_suspended_md The function dm_blk_report_zones tests if the device is suspended with the "dm_suspended_md" call. However, this function is called without holding any locks, so the device may be suspended just after it. Move the call to dm_suspended_md after dm_get_live_table, so that the device can't be suspended after the suspended state was tested.	N/A	More Details
CVE-2026-46328	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix rlimit for posix cpu timers Posix cpu timers requires an additional step beyond setting the rlimit. Refactor the code so its clear when what code is setting the limit and conditionally update the posix cpu timers when appropriate.	N/A	More Details
CVE-2026-46329	In the Linux kernel, the following vulnerability has been resolved: erofs: handle end of filesystem properly for file-backed mounts I/O requests beyond the end of the filesystem should be zeroed out, similar to loopback devices and that is what we expect.	N/A	More Details
CVE-2026-46330	In the Linux kernel, the following vulnerability has been resolved: Revert "net/smc: Introduce TCP ULP support" This reverts commit d7cd421da9da2cc7b4d25b8537f66db5c8331c40. As reported by Al Viro, the TCP ULP support for SMC is fundamentally broken. The implementation attempts to convert an active TCP socket into an SMC socket by modifying the underlying `struct file`, dentry, and inode in-place, which violates core VFS invariants that assume these structures are immutable for an open file, creating a risk of use after free errors and general system instability. Given the severity of this design flaw and the fact that cleaner alternatives (e.g., LD_PRELOAD, BPF) exist for legacy application transparency, the correct course of action is to remove this feature entirely.	N/A	More Details
CVE-2026-46282	In the Linux kernel, the following vulnerability has been resolved: iio: frequency: admv1013: fix NULL pointer dereference on str When device_property_read_string() fails, str is left uninitialized but the code falls through to strcmp(str, ...), dereferencing a garbage pointer. Replace manual read/strcmp with device_property_match_property_string() and consolidate the SE mode enums into a single sequential enum, mapping to hardware register values via a switch consistent with other bitfields in the driver. Several cleanup patches have been applied to this driver recently so this will need a manual backport.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: greybus: gb-beagleplay: bound bootloader receive buffering cc1352_bootloader_rx() appends each serdev chunk into the fixed rx_buffer before parsing bootloader packets. The helper can keep leftover bytes between callbacks and may		More

2026-46332	receive multiple packets in one callback, so a single count value is not constrained by one packet length. Check that the incoming chunk fits in the remaining receive buffer space before memcpy(). If it does not, drop the staged data and consume the bytes instead of overflowing rx_buffer.	N/A	Details
CVE-2026-47899	The Electron preload script in Logseq exposes an API method that allows the renderer process to invoke IPC handlers without proper path validation. An attacker with JavaScript execution in the renderer (e.g. via XSS or a malicious plugin), can read, write, or delete arbitrary files on the user's system. While only version v0.10.15 was tested and confirmed as vulnerable, status of other versions is unknown since this issue was not addressed by a patch.	N/A	More Details
CVE-2026-47900	Logseq is vulnerable to a stored cross-site scripting (XSS). A malicious plugin can include a JavaScript payload in the "name" field of its "package.json" file, which is rendered using "innerHTML" without proper sanitization, allowing the execution of arbitrary code in the privileged host context. While only version v0.10.15 was tested and confirmed as vulnerable, status of other versions is unknown since this issue was not addressed by a patch.	N/A	More Details
CVE-2026-47901	Logseq is vulnerable to a sandbox escape flaw where plugins running in sandboxed iframes can inject arbitrary HTML attributes, such as event handlers, into their container element in the host DOM. Due to a disabled Content Security Policy (CSP), this allows a malicious plugin to execute arbitrary JavaScript in the privileged host context, potentially gaining unauthorized access to filesystem APIs. While only version v0.10.15 was tested and confirmed as vulnerable, status of other versions is unknown since this issue was not addressed by a patch.	N/A	More Details
CVE-2026-9210	Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	N/A	More Details
CVE-2026-9211	An unauthenticated user on the local network can gain control of the router and make unauthorized changes to its operation.	N/A	More Details
CVE-2026-9212	Insufficient authentication and input validation in the listed NETGEAR models allow users connected to the local network to execute commands impacting product's confidentiality or change certain configurations.	N/A	More Details
CVE-2026-46399	HAX CMS helps manage microsite universe with PHP or NodeJs backends. The PHP version of HAX CMS prior to version 26.0.0 has an authenticated file overwrite vulnerability. An attacker can exploit this vulnerability to configure malicious Git filter commands and achieve code execution on the HAX CMS server. Version 26.0.0 patches the issue.	N/A	More Details
CVE-2026-46319	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ct: Only release RCU read lock after ct_ft When looking up a flow table in act_ct in tcf_ct_flow_table_get(), rhashtable_lookup_fast() internally opens and closes an RCU read critical section before returning ct_ft. The tcf_ct_flow_table_cleanup_work() can complete before refcount_inc_not_zero() is invoked on the returned ct_ft resulting in a UAF on the already freed ct_ft object. This vulnerability can lead to privilege escalation. Analysis from zdi-disclosures@trendmicro.com: When initializing act_ct, tcf_ct_init() is called, which internally triggers tcf_ct_flow_table_get(). static int tcf_ct_flow_table_get(struct net *net, struct tcf_ct_params *params) { struct zones_ht_key key = { .net = net, .zone = params->zone }; struct tcf_ct_flow_table *ct_ft; int err = -ENOMEM; mutex_lock(&zones_mutex); ct_ft = rhashtable_lookup_fast(&zones_ht, &key, zones_params); // [1] if (ct_ft && refcount_inc_not_zero(&ct_ft->ref)) // [2] goto out_unlock; ... } static __always_inline void *rhashtable_lookup_fast(struct rhashtable *ht, const void *key, const struct rhashtable_params params) { void *obj; rcu_read_lock(); obj = rhashtable_lookup(ht, key, params); rcu_read_unlock(); return obj; } At [1], rhashtable_lookup_fast() looks up and returns the corresponding ct_ft from zones_ht . The lookup is performed within an RCU read critical section through rcu_read_lock() / rcu_read_unlock(), which prevents the object from being freed. However, at the point of function return, rcu_read_unlock() has already been called, and there is nothing preventing ct_ft from being freed before reaching refcount_inc_not_zero(&ct_ft->ref) at [2]. This interval becomes the race window, during which ct_ft can be freed. Free Process: tcf_ct_flow_table_put() is executed through the path tcf_ct_cleanup() call_rcu() tcf_ct_params_free_rcu() tcf_ct_params_free() tcf_ct_flow_table_put(). static void tcf_ct_flow_table_put(struct tcf_ct_flow_table *ct_ft) { if (refcount_dec_and_test(&ct_ft->ref)) { rhashtable_remove_fast(&zones_ht, &ct_ft->node, zones_params); INIT_RCU_WORK(&ct_ft->rwork, tcf_ct_flow_table_cleanup_work); // [3] queue_rcu_work(act_ct_wq, &ct_ft->rwork); } } At [3], tcf_ct_flow_table_cleanup_work() is scheduled as RCU work static void tcf_ct_flow_table_cleanup_work(struct work_struct *work) { struct tcf_ct_flow_table *ct_ft; struct flow_block *block; ct_ft = container_of(to_rcu_work(work), struct tcf_ct_flow_table, rwork); nf_flow_table_free(&ct_ft->nf_ft); block = &ct_ft->nf_ft.flow_block; down_write(&ct_ft->nf_ft.flow_block_lock); WARN_ON(!list_empty(&block->cb_list)); up_write(&ct_ft->nf_ft.flow_block_lock); kfree(ct_ft); // [4] module_put(THIS_MODULE); } tcf_ct_flow_table_cleanup_work() frees ct_ft at [4]. When this function executes between [1] and [2], UAF occurs. This race condition has a very short race window,	N/A	More Details

	making it generally difficult to trigger. Therefore, to trigger the vulnerability an msleep(100) was inserted after[1]		
CVE-2026-46320	In the Linux kernel, the following vulnerability has been resolved: tap: free page on error paths in tap_get_user_xdp() tap_get_user_xdp() rejects a frame shorter than ETH_HLEN with -EINVAL, and returns -ENOMEM when build_skb() fails. Both paths jump to the err label without freeing the page that vhost_net_build_xdp() allocated for the frame. tap_sendmsg() discards the per-buffer return value and always returns 0, so vhost_tx_batch() takes the success path and never frees the page; each rejected frame in a batch leaks one page-frag chunk. Free the page on both error paths, before the skb is built. This is the tap counterpart of the same leak in tun_xdp_one().	N/A	More Details
CVE-2026-46321	In the Linux kernel, the following vulnerability has been resolved: tun: free page on short-frame rejection in tun_xdp_one() tun_xdp_one() returns -EINVAL on a frame shorter than ETH_HLEN without freeing the page that vhost_net_build_xdp() allocated for it. tun_sendmsg() discards that -EINVAL and still returns total_len, so vhost_tx_batch() takes the success path and never frees the page; each short frame in a batch leaks one page-frag chunk. A local process that can open /dev/net/tun and /dev/vhost-net can hit this path: it attaches a tun/tap device as the vhost-net backend and feeds TX descriptors whose length minus the virtio-net header is below ETH_HLEN. Each kick leaks the page-frag chunks for that batch, and a tight submission loop exhausts host memory and triggers an OOM panic. Free the page before returning -EINVAL, matching the XDP-program error path in the same function.	N/A	More Details
CVE-2026-46322	In the Linux kernel, the following vulnerability has been resolved: tun: free page on build_skb failure in tun_xdp_one() When build_skb() fails in tun_xdp_one(), the function sets ret to -ENOMEM and jumps to the out label, which returns without freeing the page that vhost_net_build_xdp() allocated for the frame. As with the short-frame rejection path, tun_sendmsg() discards the per-buffer error and still returns total_len, so vhost_tx_batch() takes the success path and never frees the page. Each build_skb() failure in a batch leaks one page-frag chunk. Free the page before taking the error path, matching the put_page() the other error exits of tun_xdp_one() already perform.	N/A	More Details
CVE-2026-46323	In the Linux kernel, the following vulnerability has been resolved: net: gro: don't merge zcopy skbs skb_gro_receive() can currently copy frags between the source and GRO skb, without checking the zerocopy status, and in particular the SKBFL_MANAGED_FRAG_REFS flag. When SKBFL_MANAGED_FRAG_REFS is set, the skb doesn't hold a reference on the pages in shinfo->frags. Appending those frags to another skb's frags without fixing up the page refcount can lead to UAF. When either the last skb in the GRO chain (the one we would append frags to) or the source skb is zerocopy, don't merge the skbs.	N/A	More Details
CVE-2026-46324	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: use list_del_rcu for netlink hooks nft_netdev_unregister_hooks and __nft_unregister_flowtable_net_hooks need to use list_del_rcu(), this list can be walked by concurrent dumpers. Add a new helper and use it consistently.	N/A	More Details
CVE-2026-43966	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') vulnerability in ninenines cowlib allows HTTP response splitting via non-VCHAR bytes in structured-fields string values. cow_http_struct_hd:escape_string/2 in cowlib only escapes \ and ", passing all other bytes through verbatim. This creates an encoder/decoder asymmetry: the matching parser accepts only printable ASCII (0x20–0x7E, excluding " and \), but the encoder emits any byte including CR and LF. An application that builds a structured HTTP header via cow_http_struct_hd:item/1 (or a higher-level wrapper such as cow_http_hd:wt_protocol/1) from attacker-controlled input can have \r\n injected into the serialized header value. Once on the wire, the injected CRLF terminates the current header and any following bytes are interpreted as a new header, enabling HTTP response splitting. This issue affects cowlib from 2.9.0.	N/A	More Details
CVE-2026-9213	A vulnerability in the affected NETGEAR gaming routers allows attackers with the ability to intercept and tamper traffic between the router and the Internet, to execute code on the device.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix iova-to-va conversion for MR page sizes != PAGE_SIZE The current implementation incorrectly handles memory regions (MRs) with page sizes different from the system PAGE_SIZE. The core issue is that rxe_set_page() is called with mr->page_size step increments, but the page_list stores individual struct page pointers, each representing PAGE_SIZE of memory. ib_sg_to_page() has ensured that when i>=1 either a) SG[i-1].dma_end and SG[i].dma_addr are contiguous or b) SG[i-1].dma_end and SG[i].dma_addr are mr->page_size aligned. This leads to incorrect iova-to-va conversion in scenarios: 1) page_size < PAGE_SIZE (e.g., MR: 4K, system: 64K): ibmr->iova = 0x181800 sg[0]: dma_addr=0x181800, len=0x800 sg[1]: dma_addr=0x173000, len=0x1000 Access iova = 0x181800 + 0x810 = 0x182010 Expected VA: 0x173010 (second SG, offset 0x10) Before fix: - index = (0x182010 >> 12) - (0x181800 >> 12) = 1 - page_offset = 0x182010 & 0xFFF = 0x10 - xarray[1] stores system page base 0x170000 - Resulting VA: 0x170000 + 0x10 = 0x170010 (wrong) 2) page_size > PAGE_SIZE (e.g., MR: 64K, system: 4K): ibmr->iova = 0x18f800 sg[0]: dma_addr=0x18f800, len=0x800 sg[1]: dma_addr=0x170000, len=0x1000		More

2026-46325	Access iova = 0x18f800 + 0x810 = 0x190010 Expected VA: 0x170010 (second SG, offset 0x10) Before fix: - index = (0x190010 >> 16) - (0x18f800 >> 16) = 1 - page_offset = 0x190010 & 0xFFFF = 0x10 - xarray[1] stores system page for dma_addr 0x170000 - Resulting VA: system page of 0x170000 + 0x10 = 0x170010 (wrong) Yi Zhang reported a kernel panic[1] years ago related to this defect. Solution: 1. Replace xarray with pre-allocated rxe_mr_page array for sequential indexing (all MR page indices are contiguous) 2. Each rxe_mr_page stores both struct page* and offset within the system page 3. Handle MR page_size != PAGE_SIZE relationships: - page_size > PAGE_SIZE: Split MR pages into multiple system pages - page_size <= PAGE_SIZE: Store offset within system page 4. Add boundary checks and compatibility validation This ensures correct iova-to-va conversion regardless of MR page size and system PAGE_SIZE relationship, while improving performance through array-based sequential access. Tests on 4K and 64K PAGE_SIZE hosts: - rdma-core/pytests $ ./build/bin/run_tests.py --dev eth0_rxe - blktest: $ TIMEOUT=30 QUICK_RUN=1 USE_RXE=1 NVMET_TRTYPES=rdma ./check nvme srp rnbd [1] https://lore.kernel.org/all/CAHj4cs9XRqE25jyVw9rj9YugffLn5+f=1znaBEnu1usLOciD+g@mail.gmail.com/T/	N/A	Details
CVE-2026-46276	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix zero-size GDS range init on RDNA4 RDNA4 (GFX 12) hardware removes the GDS, GWS, and OA on-chip memory resources. The gfx_v12_0 initialisation code correctly leaves adev->gds.gds_size, adev->gds.gws_size, and adev->gds.oa_size at zero to reflect this. amdgpu_ttm_init() unconditionally calls amdgpu_ttm_init_on_chip() for each of these resources regardless of size. When the size is zero, amdgpu_ttm_init_on_chip() forwards the call to ttm_range_man_init(), which calls drm_mm_init(mm, 0, 0). drm_mm_init() immediately fires DRM_MM_BUG_ON(start + size <= start) -- trivially true when size is zero -- crashing the kernel during modprobe of amdgpu on an RX 9070 XT. Guard against this by returning 0 early from amdgpu_ttm_init_on_chip() when size_in_page is zero. This skips TTM resource manager registration for hardware resources that are absent, without affecting any other GPU type. DRM_MM_BUG_ON() only asserts if CONFIG_DRM_DEBUG_MM is enabled in the kernel config. This is apparently rarely enabled as these chips have been in the market for over a year and this issue was only reported now. Oops-Analysis: http://oops.fenrus.org/reports/bugzilla.korg/221376/report.html (cherry picked from commit 5719ce5865279cad4fd5f01011fe037168503f2d)	N/A	More Details
CVE-2026-46277	In the Linux kernel, the following vulnerability has been resolved: mm/zone_device: do not touch device folio after calling ->folio_free() The contents of a device folio can immediately change after calling ->folio_free(), as the folio may be reallocated by a driver with a different order. Instead of touching the folio again to extract the pgmap, use the local stack variable when calling percpu_ref_put_many().	N/A	More Details
CVE-2026-28237	Unrestricted resource allocation in AMD uProf may be exploitable to consume excessive system resources, potentially leading to a loss of availability.	N/A	More Details
CVE-2026-0466	Improper access control in AMD uProf may allow a local attacker with user privileges to write to the kernel-shared memory section, potentially resulting in crash or denial of service.	N/A	More Details
CVE-2025-54509	Improper access control for register interface in the input-output memory management unit (IOMMU) could allow a privileged attacker to cause non-coherent accesses by the AMD secure processor (ASP) potentially resulting in loss of integrity.	N/A	More Details
CVE-2025-12694	A local privilege escalation vulnerability exists in Forcepoint VPN Client that allows a local non-administrative user to escalate privileges to SYSTEM. This issue affects VPN Client for Windows: versions 6.11.3 and prior.	N/A	More Details
CVE-2026-49762	Uncontrolled Resource Consumption vulnerability in the Elixir standard library's Version module allows an attacker who controls a version string to cause a denial of service through CPU and memory exhaustion. The version parser converts numeric version components (major, minor, patch and numeric pre-release/build identifiers) to integers without bounding their length. A single large all-digit component therefore forces a super-linear, non-yielding base-10 to arbitrary-precision integer conversion (String.to_integer/1, i.e. :erlang.binary_to_integer/1) that pins a BEAM scheduler, and a larger component raises an uncaught SystemLimitError that crashes the calling process. A single moderately sized string (around one megabyte) is enough; no authentication is required. This is reachable from the public entry points Version.parse/1, Version.parse!/1, Version.match?/3, Version.compare/2, and Version.parse_requirement/1, which applications routinely call on untrusted input such as HTTP parameters, dependency-manifest fields, and package metadata. This vulnerability is associated with program files lib/version.ex and program routines 'Elixir.Version.Parser':parse_digits/2. This issue affects Elixir: from 1.5.0 before 1.20.1.	N/A	More Details
CVE-2026-52904	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau: fix nvkm_device leak on aperture removal failure When aperture_remove_conflicting_pci_devices() fails during probe, the error path returns directly without unwinding the nvkm_device that was just allocated by nvkm_device_pci_new(). This leaks both the device wrapper and the pci_enable_device() reference taken inside it. Jump to the existing fail_nvkm label so nvkm_device_del() runs and balances both. The leak was	N/A	More Details

	introduced when the intermediate nvkm_device_del() between detection and aperture removal was dropped in favor of creating the pci device once.		
CVE-2026-46296	In the Linux kernel, the following vulnerability has been resolved: spi: s3c64xx: fix NULL-deref on driver unbind A change moving DMA channel allocation from probe() back to s3c64xx_spi_prepare_transfer() failed to remove the corresponding deallocation from remove(). Drop the bogus DMA channel release from remove() to avoid triggering a NULL-pointer dereference on driver unbind. This issue was flagged by Sashiko when reviewing a controller deregistration fix.	N/A	More Details
CVE-2026-0409	A NETGEAR security issue that could allow an attacker with ability to intercept and tamper with traffic between the router and the Internet to run commands on your device when the device administrator performs certain specific management actions. This issue affects NETGEAR Orbi 370 series devices before V12.1.2.7.	N/A	More Details
CVE-2026-46291	In the Linux kernel, the following vulnerability has been resolved: crypto: caam - guard HMAC key hex dumps in hash_digest_key Use print_hex_dump_devel() for dumping sensitive HMAC key bytes in hash_digest_key() to avoid leaking secrets at runtime when CONFIG_DYNAMIC_DEBUG is enabled.	N/A	More Details
CVE-2026-46292	In the Linux kernel, the following vulnerability has been resolved: pmdomain: core: Fix detach procedure for virtual devices in genpd If a device is attached to a PM domain through genpd_dev_pm_attach_by_id(), genpd calls pm_runtime_enable() for the corresponding virtual device that it registers. While this avoids boilerplate code in drivers, there is no corresponding call to pm_runtime_disable() in genpd_dev_pm_detach(). This means these virtual devices are typically detached from its genpd, while runtime PM remains enabled for them, which is not how things are designed to work. In worst cases it may lead to critical errors, like a NULL pointer dereference bug in genpd_runtime_suspend(), which was recently reported. For another case, we may end up keeping an unnecessary vote for a performance state for the device. To fix these problems, let's add this missing call to pm_runtime_disable() in genpd_dev_pm_detach().	N/A	More Details
CVE-2026-46293	In the Linux kernel, the following vulnerability has been resolved: clk: microchip: mpfs-ccc: fix out of bounds access during output registration UBSAN reported an out of bounds access during registration of the last two outputs. This out of bounds access occurs because space is only allocated in the hws array for two PLLs and the four output dividers that each has, but the defined IDs contain two DLLS and their two outputs each, which are not supported by the driver. The ID order is PLLs -> DLLs -> PLL outputs -> DLL outputs. Decrement the PLL output IDs by two while adding them to the array to avoid the problem.	N/A	More Details
CVE-2026-46294	In the Linux kernel, the following vulnerability has been resolved: dm: fix a buffer overflow in ioctl processing Tony Asleson (using Claude) found a buffer overflow in dm-ioctl in the function retrieve_status: 1. The code in retrieve_status checks that the output string fits into the output buffer and writes the output string there 2. Then, the code aligns the "outptr" variable to the next 8-byte boundary: outptr = align_ptr(outptr); 3. The alignment doesn't check overflow, so outptr could point past the buffer end 4. The "for" loop is iterated again, it executes: remaining = len - (outptr - outbuf); 5. If "outptr" points past "outbuf + len", the arithmetics wraps around and the variable "remaining" contains unusually high number 6. With "remaining" being high, the code writes more data past the end of the buffer Luckily, this bug has no security implications because: 1. Only root can issue device mapper ioctls 2. The commonly used libraries that communicate with device mapper (libdevmapper and devicemapper-rs) use buffer size that is aligned to 8 bytes - thus, "outptr = align_ptr(outptr)" can't overshoot the input buffer and the bug can't happen accidentally	N/A	More Details
CVE-2026-46295	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Do IRR scan in __kvm_apic_update_irr even if PIR is empty Fall back to apic_find_highest_vector() when PID.ON is set but PIR turns out to be empty, to correctly report the highest pending interrupt from the existing IRR. In a nested VM stress test, the following WARNING fires in vmx_check_nested_events() when kvm_cpu_has_interrupt() reports a pending interrupt but the subsequent kvm_apic_has_interrupt() (which invokes vmx_sync_pir_to_irr() again) returns -1: WARNING: CPU: 99 PID: 57767 at arch/x86/kvm/vmx/nested.c:4449 vmx_check_nested_events+0x6bf/0x6e0 [kvm_intel] Call Trace: kvm_check_and_inject_events vcpu_enter_guest.constprop.0 vcpu_run kvm_arch_vcpu_ioctl_run kvm_vcpu_ioctl __x64_sys_ioctl do_syscall_64 entry_SYSCALL_64_after_hwframe The root cause is a race between vmx_sync_pir_to_irr() on the target vCPU and __vmx_deliver_posted_interrupt() on a sender vCPU. The sender performs two individually-atomic operations that are not a single transaction: 1. pi_test_and_set_pir(vector) -- sets the PIR bit 2. pi_test_and_set_on() -- sets PID.ON The following interleaving triggers the bug: Sender vCPU (IPI): Target vCPU (1st sync_pir_to_irr): B1: set PIR[vector] A1: pi_clear_on() A2: pi_harvest_pir() -> sees B1 bit A3: xchg() -> consumes bit, PIR=0 (1st sync returns correct max_irr) B2: set PID.ON = 1 Target vCPU (2nd sync_pir_to_irr): C1: pi_test_on() -> TRUE (from B2) C2: pi_clear_on() -> ON=0 C3: pi_harvest_pir() -> PIR empty C4: *max_irr = -1, early return IRR NOT SCANNED The interrupt is not lost (it resides in the IRR from the first sync and is recovered on the next vcpu_enter_guest() iteration), but the incorrect max_irr causes a spurious WARNING and a wasted L2 VM-Enter/VM-Exit cycle.	N/A	More Details

CVE-2026-46297	In the Linux kernel, the following vulnerability has been resolved: net: libwx: use request_irq for VF misc interrupt Currently, request_threaded_irq() is used with a primary handler but a NULL threaded handler, while also setting the IRQF_ONESHOT flag. This specific combination triggers a WARNING since the commit aef30c8d569c ("genirq: Warn about using IRQF_ONESHOT without a threaded handler"). WARNING: kernel/irq/manage.c:1502 at __setup_irq+0x4fa/0x760 Fix the issue by switching to request_irq(), which is the appropriate interface or a non-threaded interrupt handler, and removing the unnecessary IRQF_ONESHOT flag.	N/A	More Details
CVE-2026-46290	In the Linux kernel, the following vulnerability has been resolved: x86/efi: Fix graceful fault handling after FPU softirq changes Since commit d02198550423 ("x86/fpu: Improve crypto performance by making kernel-mode FPU reliably usable in softirqs"), kernel_fpu_begin() calls fpregs_lock() which uses local_bh_disable() instead of the previous preempt_disable(). This sets SOFTIRQ_OFFSET in preempt_count during the entire EFI runtime service call, causing in_interrupt() to return true in normal task context. The graceful page fault handler efi_crash_gracefully_on_page_fault() uses in_interrupt() to bail out for faults in real interrupt context. With SOFTIRQ_OFFSET now set, the handler always bails out, leaving EFI firmware page faults unhandled. This escalates to die() which also sees in_interrupt() as true and calls panic("Fatal exception in interrupt"), resulting in a hard system freeze. On systems with buggy firmware that triggers page faults during EFI runtime calls (e.g., accessing unmapped memory in GetTime()), this causes an unrecoverable hang instead of the expected graceful EFI_ABORTED recovery. Fix by replacing in_interrupt() with !in_task(). This preserves the original intent of bailing for interrupts or NMI faults, while no longer falsely triggering from the FPU code path's local_bh_disable(). [ardb: Sashiko spotted that using 'in_hardirq() || in_nmi()' leaves a window where a softirq may be taken before fpregs_lock() is called, but after efi_rts_work.efi_rts_id has been assigned, and any page faults occurring in that window will then be misidentified as having been caused by the firmware. Instead, use !in_task(), which incorporates in_serving_softirq().]	N/A	More Details
CVE-2026-46298	In the Linux kernel, the following vulnerability has been resolved: pseries/papr-hvpipe: Fix race with interrupt handler While executing ->ioctl handler or ->release handler, if an interrupt fires on the same cpu, then we can enter into a deadlock. This patch fixes both these handlers to take spin_lock_irq{save|restore} versions of the lock to prevent this deadlock.	N/A	More Details
CVE-2026-46299	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix held lock freed on hfsplus_fill_super() hfsplus_fill_super() calls hfs_find_init() to initialize a search structure, which acquires tree->tree_lock. If the subsequent call to hfsplus_cat_build_key() fails, the function jumps to the out_put_root error label without releasing the lock. The later cleanup path then frees the tree data structure with the lock still held, triggering a held lock freed warning. Fix this by adding the missing hfs_find_exit(&fd) call before jumping to the out_put_root error label. This ensures that tree->tree_lock is properly released on the error path. The bug was originally detected on v6.13-rc1 using an experimental static analysis tool we are developing, and we have verified that the issue persists in the latest mainline kernel. The tool is specifically designed to detect memory management issues. It is currently under active development and not yet publicly available. We confirmed the bug by runtime testing under QEMU with x86_64 defconfig, lockdep enabled, and CONFIG_HFSPLUS_FS=y. To trigger the error path, we used GDB to dynamically shrink the max_unistr_len parameter to 1 before hfsplus_asc2uni() is called. This forces hfsplus_asc2uni() to naturally return -ENAMETOOLONG, which propagates to hfsplus_cat_build_key() and exercises the faulty error path. The following warning was observed during mount: ========== WARNING: held lock freed! 7.0.0-rc3-00016-gb4f0dd314b39 #4 Not tainted ---------- mount/174 is freeing memory ffff888103f92000-ffff888103f92fff, with a lock still held there! ffff888103f920b0 (&tree->tree_lock){+.+.}-{4:4}, at: hfsplus_find_init+0x154/0x1e0 2 locks held by mount/174: #0: ffff888103f960e0 (&type->s_umount_key#42/1){+.+.}-{4:4}, at: alloc_super.constprop.0+0x167/0xa40 #1: ffff888103f920b0 (&tree->tree_lock){+.+.}-{4:4}, at: hfsplus_find_init+0x154/0x1e0 stack backtrace: CPU: 2 UID: 0 PID: 174 Comm: mount Not tainted 7.0.0-rc3-00016-gb4f0dd314b39 #4 PREEMPT(lazy) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x82/0xd0 debug_check_no_locks_freed+0x13a/0x180 kfree+0x16b/0x510 ? hfsplus_fill_super+0xcb4/0x18a0 hfsplus_fill_super+0xcb4/0x18a0 ? __pfx_hfsplus_fill_super+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? bdev_open+0x65f/0xc30 ? srso_return_thunk+0x5/0x5f ? pointer+0x4ce/0xbf0 ? trace_contention_end+0x11c/0x150 ? __pfx_pointer+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? bdev_open+0x79b/0xc30 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? vsnprintf+0x6da/0x1270 ? srso_return_thunk+0x5/0x5f ? __mutex_unlock_slowpath+0x157/0x740 ? __pfx_vsnprintf+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? mark_held_locks+0x49/0x80 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? irqentry_exit+0x17b/0x5e0 ? trace_irq_disable.constprop.0+0x116/0x150 ? __pfx_hfsplus_fill_super+0x10/0x10 ? __pfx_hfsplus_fill_super+0x10/0x10 get_tree_bdev_flags+0x302/0x580 ? __pfx_get_tree_bdev_flags+0x10/0x10 ? vfs_parse_fs_qstr+0x129/0x1a0 ? __pfx_vfs_parse_fs_qstr+0x3/0x10 vfs_get_tree+0x89/0x320 fc_mount+0x10/0x1d0 path_mount+0x5c5/0x21c0 ? __pfx_path_mount+0x10/0x10 ? trace_irq_enable.constprop.0+0x116/0x150 ? trace_irq_enable.constprop.0+0x116/0x150 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? kmem_cache_free+0x307/0x540 ? user_path_at+0x51/0x60 ? __x64_sys_mount+0x212/0x280 ? srso_return_thunk+0x5/0x5f	N/A	More Details

	__x64_sys_mount+0x212/0x280 ? __pfx___x64_sys_mount+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? trace_irq_enable.constprop.0+0x116/0x150 ? srso_return_thunk+0x5/0x5f do_syscall_64+0x111/0x680 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7ffacad55eae Code: 48 8b 0d 85 1f 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 a5 00 00 8 RSP: 002b ---truncated---		
CVE-2026-46301	In the Linux kernel, the following vulnerability has been resolved: spi: topcliff-pch: fix use-after-free on unbind Give the driver a chance to flush its queue before releasing the DMA buffers on driver unbind	N/A	More Details
CVE-2026-46302	In the Linux kernel, the following vulnerability has been resolved: selinux: allow multiple opens of /sys/fs/selinux/policy Currently there can only be a single open of /sys/fs/selinux/policy at any time. This allows any process to block any other process from reading the kernel policy. The original motivation seems to have been a mix of preventing an inconsistent view of the policy size and preventing userspace from allocating kernel memory without bound, but this is arguably equally bad. Eliminate the policy_opened flag and shrink the critical section that the policy mutex is held. While we are making changes here, drop a couple of extraneous BUG_ONs.	N/A	More Details
CVE-2026-0410	Authenticated administrators connected to the local network can gain elevated access to the router and make unauthorized changes to router software and functionality.	N/A	More Details
CVE-2026-46303	In the Linux kernel, the following vulnerability has been resolved: isofs: validate Rock Ridge CE continuation extent against volume size rock_continue() reads rs->cont_extent verbatim from the Rock Ridge CE record and passes it to sb_bread() without checking that the block number is within the mounted ISO 9660 volume. commit e595447e177b ("[PATCH] rock.c: handle corrupted directories") added cont_offset and cont_size rejection for the CE continuation but did not validate the extent block number itself. commit f54e18f1b831 ("isofs: Fix infinite looping over CE entries") later capped the CE chain length at RR_MAX_CE_ENTRIES = 32 but again left the block number unchecked. With a crafted ISO mounted via udisks2 (desktop optical auto-mount) or via CAP_SYS_ADMIN mount, rs->cont_extent can therefore point at an out-of-range block or at blocks belonging to an adjacent filesystem on the same block device. sb_bread() on an out-of-range block returns NULL cleanly via the block layer EIO path, so there is no memory-safety violation. For in-range reads of adjacent- filesystem data, the CE buffer is parsed as Rock Ridge records and only the text of SL sub-records reaches userspace through readlink(), which makes the info-leak channel narrow and difficult to exploit; still, rejecting the malformed CE outright matches the rejection shape already present in the same function for cont_offset and cont_size. Add an ISOFS_SB(sb)->s_nzones bounds check to rock_continue() next to the existing offset/size rejection, printing the same corrupted-directory-entry notice.	N/A	More Details
CVE-2026-8045	CWE-611 Improper Restriction of XML External Entity Reference vulnerability exists that could cause information disclosure of server-side file contents when an attacker with a Data Center Expert user account submits crafted XML payloads to SOAP service endpoints.	N/A	More Details
CVE-2026-46289	In the Linux kernel, the following vulnerability has been resolved: lib/scatterlist: fix length calculations in extract_kvec_to_sg Patch series "Fix bugs in extract_iter_to_sg()", v3. Fix bugs in the kvec and user variants of extract_iter_to_sg. This series is growing due to useful remarks made by sashiko.dev. The main bugs are: - The length for an sglist entry when extracting from a kvec can exceed the number of bytes in the page. This is obviously not intended. - When extracting a user buffer the sglist is temporarily used as a scratch buffer for extracted page pointers. If the sglist already contains some elements this scratch buffer could overlap with existing entries in the sglist. The series adds test cases to the kunit_iov_iter test that demonstrate all of these bugs. Additionally, there is a memory leak fix for the test itself. The bugs were orignally introduced into kernel v6.3 where the function lived in fs/netfs/iterator.c. It was later moved to lib/scatterlist.c in v6.5. Thus the actual fix is only marked for backports to v6.5+. This patch (of 5): When extracting from a kvec to a scatterlist, do not cross page boundaries. The required length was already calculated but not used as intended. Adjust the copied length if the loop runs out of sglist entries without extracting everything. While there, return immediately from extract_iter_to_sg if there are no sglist entries at all. A subsequent commit will add kunit test cases that demonstrate that the patch is necessary.	N/A	More Details
CVE-2026-52905	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: disallow non-power of two min_region_sz on damon_start() Commit d8f867fa0825 ("mm/damon: add damon_ctx->min_sz_region") introduced a bug that allows unaligned DAMON region address ranges. Commit c80f46ac228b ("mm/damon/core: disallow non-power of two min_region_sz") fixed it, but only for damon_commit_ctx() use case. Still, DAMON sysfs interface can emit non-power of two min_region_sz via damon_start(). Fix the path by adding the is_power_of_2() check on damon_start(). The issue was discovered by sashiko [1].	N/A	More Details
	Waves Central for macOS versions 13.0.9 through 16.5.5 contain a local privilege escalation vulnerability. A trusted XPC client component included with the product is signed with hardened runtime entitlements		

CVE-2026-24064	that permit dynamic library injection. A local attacker can set the DYLD_INSERT_LIBRARIES environment variable to inject an attacker-controlled dynamic library into the trusted client process at launch. The injected code runs within the signed process and can connect to the product's privileged helper service to invoke privileged operations, resulting in arbitrary code execution as root. The issue is fixed in version 16.6.2.	N/A	More Details
CVE-2026-52906	In the Linux kernel, the following vulnerability has been resolved: 9p: fix access mode flags being ORed instead of replaced Since commit 1f3e4142c0eb ("9p: convert to the new mount API"), v9fs_apply_options() applies parsed mount flags with |= onto flags already set by v9fs_session_init(). For 9P2000.L, session_init sets V9FS_ACCESS_CLIENT as the default, so when the user mounts with "access=user", both bits end up set. Access mode checks compare against exact values, so having both bits set matches neither mode. This causes v9fs_fid_lookup() to fall through to the default switch case, using INVALID_UID (nobody/65534) instead of current_fsuid() for all fid lookups. Root is then unable to chown or perform other privileged operations. Fix by clearing the access mask before applying the user's choice.	N/A	More Details
CVE-2026-52907	In the Linux kernel, the following vulnerability has been resolved: media: rockchip: rkcif: fix off by one bugs Change these comparisons from > vs >= to avoid accessing one element beyond the end of the arrays. While at it, use ARRAY_SIZE instead of the _MAX enum values. [fix cosmetic issues]	N/A	More Details
CVE-2026-9279	Logseq exposes an IPC handler that allows the renderer process to execute shell commands. While an allowlist restricts the command name (e.g. `git`, `pandoc`, `grep`), the argument string is concatenated with the command and passed to `child_process.spawn` with the `shell: true` option, allowing shell metacharacters in the arguments to bypass the allowlist. An attacker with JavaScript execution in the renderer (e.g. via XSS or a malicious plugin) can execute arbitrary shell commands with the privileges of the Logseq process, leading to remote code execution on the host. While only version v0.10.15 was tested and confirmed as vulnerable, status of other versions is unknown since this issue was not addressed by a patch.	N/A	More Details
CVE-2026-46496	HAX CMS helps manage microsite universe with PHP or NodeJs backends. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 26.0.0 due to improper sanitization of the `<video-player>` component. The component allows `javascript:` URIs in the `source` attribute, which are executed when the page is viewed. This enables attackers to execute arbitrary JavaScript in the context of the victim’s browser and access sensitive data such as JWT tokens and more. Version 26.0.0 fixes the issue.	N/A	More Details
CVE-2026-45431	This vulnerability exists in GX Earth ONT models due to improper handling of user-supplied input in multiple diagnostic functions in its web management interface. An authenticated remote attacker could exploit this vulnerability by injecting arbitrary and executing OS commands on the targeted device. Successful exploitation of this vulnerability could allow the attacker to perform remote code execution with root privileges on the targeted device.	N/A	More Details
CVE-2026-45432	This vulnerability exists in GX Earth ONT models due to the transmission of user credentials in plaintext over HTTP in its web management interface. A remote attacker could exploit this vulnerability by intercepting network traffic to obtain sensitive authentication information, which could lead to unauthorized access to the targeted device.	N/A	More Details
CVE-2026-46283	In the Linux kernel, the following vulnerability has been resolved: tpm: Use kfree_sensitive() to free auth session in tpm_dev_release() tpm_dev_release() uses plain kfree() to free chip->auth, which contains sensitive cryptographic material including HMAC session keys, nonces, and passphrase data (struct tpm2_auth). Every other code path that frees this structure uses kfree_sensitive() to zero the memory before releasing it: both tpm2_end_auth_session() and tpm_buf_check_hmac_response() do so. The tpm_dev_release() path is the only one that does not, leaving key material in freed slab memory until it is eventually overwritten. Use kfree_sensitive() for consistency with the rest of the driver and to ensure session keys are scrubbed during device teardown.	N/A	More Details
CVE-2026-46288	In the Linux kernel, the following vulnerability has been resolved: of: unittest: fix use-after-free in of_unittest_changeset() The variable 'parent' is assigned the value of 'nchangeset' earlier in the function, meaning both point to the same struct device_node. The call to of_node_put(nchangeset) can decrement the reference count to zero and free the node if there are no other holders. After that, the code still uses 'parent' to check for the presence of a property and to read a string property, leading to a use-after-free. Fix this by moving the of_node_put() call after the last access to 'parent', avoiding the UAF.	N/A	More Details
CVE-2026-26236	A missing authorization vulnerability has been reported to affect QuMagie. The remote attackers can then exploit the vulnerability to access unauthorized data or perform unauthorized actions. We have already fixed the vulnerability in the following version: QuMagie 2.9.0 and later	N/A	More Details
CVE-2026-46284	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix early boot crash on parameters without '=' separator If hugepages, hugepagesz, or default_hugepagesz are specified on the kernel command line without the '=' separator, early parameter parsing passes NULL to hugetlb_add_param(), which dereferences it in strlen() and can crash the system during early boot. Reject	N/A	More Details

	NULL values in hugetlb_add_param() and return -EINVAL instead.		
CVE-2026-11347	The linqi application contains hardcoded cryptographic keys. Additionally, the application uses a weak algorithm with a limited ASCII charset to dynamically generate Initialization Vectors (IVs) for AES/CBC encryption, making known-plaintext attacks feasible. An attacker with local access can leverage these vulnerabilities to decrypt sensitive obfuscated strings, including ConnectionString values containing database credentials from appsettings.json.	N/A	More Details
CVE-2026-46285	In the Linux kernel, the following vulnerability has been resolved: mtd: docg3: fix use-after-free in docg3_release() In docg3_release(), the docg3 pointer is obtained from cascade->floors[0]->priv before the loop that calls doc_release_device() on each floor. doc_release_device() frees the docg3 struct via kfree(docg3) at line 1881. After the loop, docg3->cascade->bch dereferences the already-freed pointer. Fix this by accessing cascade->bch directly, which is equivalent since docg3->cascade points back to the same cascade struct, and is already available as a local variable. This also removes the now-unused docg3 local variable.	N/A	More Details
CVE-2026-46286	In the Linux kernel, the following vulnerability has been resolved: leds: qcom-lpg: Check for array overflow when selecting the high resolution When selecting the high resolution values from the array, FIELD_GET() is used to pull from a 3 bit register, yet the array being indexed has only 5 values in it. Odds are the hardware is sane, but just to be safe, properly check before just overflowing and reading random data and then setting up chip values based on that.	N/A	More Details
CVE-2026-46287	In the Linux kernel, the following vulnerability has been resolved: net: txgbe: fix RTNL assertion warning when remove module For the copper NIC with external PHY, the driver called phylink_connect_phy() during probe and phylink_disconnect_phy() during remove. It caused an RTNL assertion warning in phylink_disconnect_phy() upon module remove. To fix this, add rtnl_lock() and rtnl_unlock() around the phylink_disconnect_phy() in remove function. ------------[cut here]------------ RTNL: assertion failed at drivers/net/phy/phylink.c (2351) WARNING: drivers/net/phy/phylink.c:2351 at phylink_disconnect_phy+0xd8/0xf0 [phylink], CPU#0: rmmod/4464 Modules linked in: ... CPU: 0 UID: 0 PID: 4464 Comm: rmmod Kdump: loaded Not tainted 7.0.0-rc4+ Hardware name: Micro-Star International Co., Ltd. MS-7E16/X670E GAMING PLUS WIFI (MS-7E16), BIOS 1.90 12/31/2024 RIP: 0010:phylink_disconnect_phy+0xe4/0xf0 [phylink] Code: 5b 41 5c 41 5d 41 5e 41 5f 5d 31 c0 31 d2 31 f6 31 ff e9 3a 38 8f e7 48 8d 3d 48 87 e2 ff ba 2f 09 00 00 48 c7 c6 c1 22 24 c0 <67> 48 0f b9 3a e9 34 ff ff ff 66 90 90 90 90 90 90 90 90 90 90 90 RSP: 0018:ffffce7288363ac0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff89654b2a1a00 RCX: 0000000000000000 RDX: 000000000000092f RSI: ffffffffc02422c1 RDI: ffffffffc0239020 RBP: ffffce7288363ae8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8964c4022000 R13: ffff89654fce3028 R14: ffff89654ebb4000 R15: ffffffffc0226348 FS: 0000795e80d93780(0000) GS:ffff896c52857000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00005b528b592000 CR3: 0000000170d0f000 CR4: 0000000000f50ef0 PKRU: 55555554 Call Trace: <TASK> txgbe_remove_phy+0xbb/0xd0 [txgbe] txgbe_remove+0x4c/0xb0 [txgbe] pci_device_remove+0x41/0xb0 device_remove+0x43/0x80 device_release_driver_internal+0x206/0x270 driver_detach+0x4a/0xa0 bus_remove_driver+0x83/0x120 driver_unregister+0x2f/0x60 pci_unregister_driver+0x40/0x90 txgbe_driver_exit+0x10/0x850 [txgbe] __do_sys_delete_module.isra.0+0x1c3/0x2f0 __x64_sys_delete_module+0x12/0x20 x64_sys_call+0x20c3/0x2390 do_syscall_64+0x11c/0x1500 ? srso_alias_return_thunk+0x5/0xfbef5 ? do_syscall_64+0x15a/0x1500 ? srso_alias_return_thunk+0x5/0xfbef5 ? do_fault+0x312/0x580 ? srso_alias_return_thunk+0x5/0xfbef5 ? __handle_mm_fault+0x9d5/0x1040 ? srso_alias_return_thunk+0x5/0xfbef5 ? count_memcg_events+0x101/0x1d0 ? srso_alias_return_thunk+0x5/0xfbef5 ? handle_mm_fault+0x1e8/0x2f0 ? srso_alias_return_thunk+0x5/0xfbef5 ? do_user_addr_fault+0x2f8/0x820 ? srso_alias_return_thunk+0x5/0xfbef5 ? irqentry_exit+0xb2/0x600 ? srso_alias_return_thunk+0x5/0xfbef5 ? exc_page_fault+0x92/0x1c0 entry_SYSCALL_64_after_hwframe+0x76/0x7e	N/A	More Details
CVE-2026-7774	tarfile.data_filter could be bypassed using crafted link entries, including symlinks with empty or directory-like names, to redirect later archive members outside the intended extraction directory. This allowed a malicious tar archive to cause tarfile.extractall() to write files outside the destination directory, subject to the permissions of the extracting process.	N/A	More Details