SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 September 2026

Generated on 09 September 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-2026-86152	A flaw has been found in Tenda CP3 27.5.57.101. The impacted element is the function CAutoAddWifi::ThreadProc of the file Functions/AutoAddWifi.cpp of the component Kylin. Executing a manipulation can lead to os command injection. The attack may be launched remotely.	10.0	More Details
CVE-2026-70352	Missing authentication for critical function in Azure AI Language allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-44756	A memory safety vulnerability exists in the Extended Passport Protocol (EPP) processing library. Under specific conditions, an unauthenticated attacker could exploit a crafted network request containing a malformed EPP header, potentially resulting in undefined behavior and abnormal program termination. Successful exploitation may have a high impact on the confidentiality, integrity, and availability of the application.	10.0	More Details
CVE-2026-85061	MapLibre GL JS is an interactive vector tile map library for web browsers. Prior to 6.4.1, DOM.sanitize() in src/util/dom.ts iterates elem.attributes as a live NamedNodeMap while removeAttributes() removes attributes from the same collection, shifting indexes and skipping an adjacent dangerous attribute. An attacker who controls untrusted third-party style attribution strings or user-supplied custom attributions can supply consecutive dangerous attributes, causing an attribute such as onload or ontoggle to survive sanitization and execute when the attribution control inserts the content into innerHTML. A victim must render the affected map content for the script to execute. This issue is fixed in version 6.4.1.	10.0	More Details
CVE-2026-75650	Adobe Commerce is affected by an Improper Neutralization of Special Elements Used in a Template Engine vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	10.0	More Details
CVE-2026-83711	Authorization bypass through user-controlled key in Microsoft Azure Active Directory B2C allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-86296	A vulnerability was determined in D-Link DIR-822A A_101. This vulnerability affects the function strcpy of the file udhcpcd/serverpacket.c of the component udhcpcd. This manipulation causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	10.0	More Details

CVE-2026-4357	The Embed HTML5 Game WordPress plugin through 1.3 does not properly restrict who can upload files via the plugin, as well as what can be uploaded, making it possible for unauthenticated attackers to upload PHP backdoors on affected sites.	10.0	More Details
CVE-2026-86510	A vulnerability has been found in D-Link DIR-822A A_101. Affected is the function tunnel_set_params of the component L2TP Control Message Parser. Such manipulation leads to out-of-bounds write. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	9.9	More Details
CVE-2026-79697	A vulnerability was determined in Advantech WISE-6610-NB, WISE-6610-EB, WISE-6610-TB, WISE-6610-JB, WISE-6610-CB, WISE-6610-EL-NB, WISE-6610-EL-EB, WISE-6610-EL-TB, WISE-6610-EL-JB, WISE-6610-EL-CB, WISE-6610P-DEA, WISE-6610P-DNA and WISE-6610P-DTA 1.2.1_20251110. This affects the function basicstation_apply of the component Basic Station Certificate-Deletion Handler. This manipulation of the argument act causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.2.4_20260821 is able to mitigate this issue. Upgrading the affected component is advised. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	9.9	More Details
CVE-2026-85031	A vulnerability was found in TOTOLINK CP450 4.1.0. The impacted element is an unknown function of the file /cgi-bin/cstecgi.cgi. Performing a manipulation of the argument topicurl results in buffer overflow. Remote exploitation of the attack is possible.	9.9	More Details
CVE-2026-78234	A flaw was found in hawtio-operator. The operator reads the OpenShift Service CA private signing key from the openshift-service-ca namespace and uses it to mint client certificates with a Subject Common Name (CN) supplied by the author of a namespaced Hawtio custom resource. Because the operator ships a ClusterRole that aggregates Hawtio CR permissions into the edit and admin roles, any user with edit access in any namespace can obtain a Service-CA-signed certificate with an arbitrary subject. This certificate can be used to impersonate any in-cluster service identity to peers that trust the Service CA for client authentication, including Jolokia agents and other Service-CA-trusting components.	9.9	More Details
CVE-2026-85223	A vulnerability was found in D-Link DNS-340L 1.01B04. Affected by this issue is some unknown functionality of the file /cgi-bin/dropbox.cgi of the component CGI Handler. Performing a manipulation of the argument callback_url/sync_interval results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used.	9.9	More Details
CVE-2026-12645	A Missing Authorization vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.	9.9	More Details
CVE-2026-12646	A Missing Authorization vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.	9.9	More Details
CVE-2026-79698	A vulnerability was identified in Advantech WISE-6610-NB, WISE-6610-EB, WISE-6610-TB, WISE-6610-JB, WISE-6610-CB, WISE-6610-EL-NB, WISE-6610-EL-EB, WISE-6610-EL-TB, WISE-6610-EL-JB, WISE-6610-EL-CB, WISE-6610P-DEA, WISE-6610P-DNA and WISE-6610P-DTA 1.2.1_20251110. This vulnerability affects the function nodered_lib_apply of the component Node-RED Library. Such manipulation of the argument act leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. Upgrading to version 1.2.4_20260821 is able to resolve this issue. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	9.9	More Details
CVE-2026-86167	A vulnerability was identified in Tenda HG10 300001138. Impacted is the function formgponConf of the file /boaform/admin/formgponConf of the component Boa. The manipulation of the argument fmgpon_loid leads to os command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	9.9	More Details
CVE-2026-12647	A Missing Authorization vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.	9.9	More Details
CVE-2026-12650	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.	9.9	More Details
CVE-2026-86299	A vulnerability was detected in Linksys RE7000 2.0.15. This affects the function platform_event_pingTest of the file /cgi-bin/json.cgi?PingTest of the component PingTest Handler. The manipulation of the argument pingTestIp/pingTestPktSize/pingTestTimes results in os command injection. The attack can be launched remotely. The exploit is now public and may be used.	9.9	More Details
CVE-2026-26084	A improper access control vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox Cloud 5.0.4 through 5.0.5, FortiSandbox PaaS 5.0.4 through 5.0.5 may allow attacker to access sensitive information via crafted HTTP requests.	9.9	More Details

CVE-2026-77009	The WatchMan-Site7 WordPress plugin through 4.2.0 does not restrict access to its debugging console, which executes user-supplied PHP code, allowing any authenticated user, such as a subscriber, to run arbitrary code on the server.	9.9	More Details
CVE-2026-85672	zerox 1.1.20 contains an OS command injection vulnerability in the file download mechanism where the temporary file extension derived from document URLs is interpolated unsanitized into shell commands executed by poppler utilities. Attackers can craft document URLs with malicious file extensions containing command substitution syntax to execute arbitrary OS commands before document processing occurs.	9.8	More Details
CVE-2026-82923	The AI Website Builder WordPress plugin (GitHub build) 1.0.0 does not perform any authorisation or nonce check on its REST API routes, allowing unauthenticated attackers to install and activate plugins and themes, import content from a URL under their control, write a file of their choosing into the uploads directory, and delete site content and media. On a host that serves PHP from the uploads directory, that file write is remote code execution.	9.8	More Details
CVE-2026-85663	Aim 3.29.1 remote tracking server fails to authenticate requests and dispatches arbitrary methods through getattr without allowlist validation. Unauthenticated attackers can register clients, instantiate Repo resources, and invoke arbitrary methods to read experiments or delete runs.	9.8	More Details
CVE-2026-85661	excel-mcp-server 0.1.8 fails to enforce path confinement in stdio mode when EXCEL_FILES_PATH is unset, allowing attackers to read and write arbitrary files. Attackers can supply unchecked file paths to read and write tools to access any file accessible to the process.	9.8	More Details
CVE-2026-85148	SmartIT Desktop Manager developed by Lightstar has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can exploit a fixed password to remotely access user hosts.	9.8	More Details
CVE-2026-85504	FreeIPMI before 1.6.19 has a stack-based buffer overflow in _ipmi_sel_oem_fujitsu_get_sel_entry_long_text in libfreeipmi/sel/ipmi-sel-string-fujitsu-irmc-common.c via malformed Fujitsu SEL long-text responses.	9.8	More Details
CVE-2026-11613	The Divi Ajax Filter plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.1.2 via the 'custom_loop_template' parameter parameter. 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. This vulnerability is only exploitable when the loop_templates parameter is set to 'custom-template'.	9.8	More Details
CVE-2026-85506	ipmi-oem in FreeIPMI before 1.6.19 has a stack-based buffer overflow in _get_dell_system_info_idrac_info in ipmi-oem/ipmi-oem-dell.c (idrac-info subcommand to dell get-system-info).	9.8	More Details
CVE-2026-85507	ipmi-oem in FreeIPMI before 1.6.19 has a stack-based buffer overflow in _output_dell_system_info_cmc_info in ipmi-oem/ipmi-oem-dell.c (cmc-info subcommand to dell get-system-info).	9.8	More Details
CVE-2026-85508	ipmi-oem in FreeIPMI before 1.6.19 has a stack-based buffer overflow in _output_dell_system_info_cmc_ipv6_info in ipmi-oem/ipmi-oem-dell.c (cmc-ipv6-info subcommand to dell get-system-info).	9.8	More Details
CVE-2026-85509	FreeIPMI before 1.6.19 has a stack-based buffer overflow in _read_fru_data in libfreeipmi/fru/ipmi-fru.c when a BMC returns more bytes than requested.	9.8	More Details
CVE-2026-15354	The ACPT (Premium) plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.0.66. This is due to missing authorization in the `submit()` function, which allows unauthenticated form submissions to control the target user ID before calling `wp_update_user()`. This makes it possible for unauthenticated attackers to overwrite any WordPress user's email address and password, including an administrator's, and take over the account. Successful exploitation requires a public ACPT user form that permits anonymous submissions.	9.8	More Details
CVE-2026-86304	MojoX::Authentication versions before 0.006 for Perl allow SAML authentication bypass because parse_assertion builds Net::SAML2::Binding::POST without a trust anchor. parse_assertion in MojoX::Authentication::Model::SAML2 calls Net::SAML2::Binding::POST->new with no cacert, cert_text or anchors argument, then passes the returned XML to Net::SAML2::Protocol::Assertion->new_from_xml with the IdP signing certificate as cacert. In Net::SAML2 before 0.86 that certificate guards only encrypted assertions, so the signature on an unencrypted assertion is checked against the certificate the response itself carries. An attacker starts a SAML login, then posts a response signed with a certificate of their own. The audience, InResponseTo and timestamp checks that follow are all satisfiable by the attacker, so the response authenticates any NameID it carries.	9.8	More Details
CVE-2026-	TEN Framework 0.11.71 contains unauthenticated arbitrary file read and write vulnerabilities in the TMAN Designer file-content API endpoints. Attackers can submit POST and PUT requests to the /api/designer/v1/file-		More

85688	content endpoints to read arbitrary files or write malicious content to system paths, enabling code execution through authorized_keys, cron files, or executable graph files.	9.8	Details
CVE-2026-86219	Authen::SASL::Perl::DIGEST_MD5 versions before 2.2100 for Perl accept replayed authentication responses via unverified nonce in server_step. server_start generates a fresh nonce and sends it in the challenge, and nothing later compares that value against the nonce the client returns. server_step derives the expected digest from the client's own parameters, so a response verifies whenever its digest matches the nonce it carries. The count table it also checks is keyed on the client-supplied nonce and starts empty in each new server object, so a captured first response, carrying `nc=00000001`, passes that too. RFC 2831 defines the nonce in the response as the value the server sent in the preceding challenge. An attacker who observes one successful `qop=auth` exchange can replay the captured response against a later session for the same service, host, realm and user, and authenticate as that user without knowing the password.	9.8	More Details
CVE-2026-16310	The MemberDash plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.8.5 via the 'id' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to change the password of any WordPress user, including administrators, by supplying an arbitrary user ID during registration, and take over their account without any notification sent to the victim.	9.8	More Details
CVE-2026-86121	Cua computer-server versions before 0.3.42 skip authentication when the CONTAINER_NAME environment variable is unset and bind to all interfaces by default, allowing unauthenticated attackers to execute arbitrary commands. Attackers can reach TCP port 8000 to run shell commands via the run_command endpoint, read and write arbitrary files through file operation endpoints, and access interactive PTY shells without authentication.	9.8	More Details
CVE-2024-11080	The Post Grid and Gutenberg Blocks – ComboBlocks plugin for WordPress is vulnerable to Unauthenticated Hook Injection in versions 2.2.32 to 2.3.1 via several functions in the ~/includes/blocks/form-wrap/function.php file. This makes it possible for unauthenticated attackers to execute actions with hooks in WordPress, granted no other security controls are present in the function.	9.8	More Details
CVE-2026-78362	The SEO Flow by LupsOnline WordPress plugin before 3.0.3 does not correctly validate the credential supplied with its API requests, allowing unauthenticated users to be served as the administrator who configured the SEO Flow by LupsOnline WordPress plugin before 3.0.3 and take over the site. Exploitation requires the SEO Flow by LupsOnline WordPress plugin before 3.0.3 to have been configured, which is its normal operating state.	9.8	More Details
CVE-2026-83627	The Hummingbird – Speed Optimization, Caching, Minify, Compress & CDN plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.21.0 via the log_msg() function in core/modules/class-page-cache.php. The page-cache debug log is written to wp-content/wphb-logs/page-caching-log.php, a directly web-accessible PHP file that is supposed to be protected by a leading '<?php die(); ?>' header. That header is guarded by class_exists('Filesystem'), which can never match because class_exists() resolves string arguments in the global namespace while the class is Hummingbird\Core\Filesystem; when the log is created during a front-end request the header is therefore omitted entirely. get_cookies() then writes the raw name of any cookie matching the wphb_cache_ prefix into that file without sanitization. This makes it possible for unauthenticated attackers to write arbitrary PHP into the log file with a single anonymous request and execute it by requesting the file directly, resulting in full remote code execution. Exploitation requires the site administrator to have enabled Page Caching with the Debug Log option (non-default), and the log file to be created during a front-end request — a state reached by the plugin's own 'Clear logs' action, any cache flush, or unattended via the plugin's daily log-rotation cron, which can strip the protective header from an existing log file.	9.8	More Details
CVE-2026-13447	The Mstore Api plugin for WordPress is vulnerable to Authentication Bypass via JWT Forgery in versions up to, and including, 4.20.0 This is due to missing cryptographic signature verification in the FirebasePhoneAuthHelper::verify_id_token() function, which decodes and validates Firebase ID token claims (alg, kid, aud, iss) but never calls openssl_verify() or any equivalent to validate the JWT signature against Google's actual public key certificates. This makes it possible for unauthenticated attackers to forge a Firebase Phone Auth JWT signed with a self-generated RSA key pair and impersonate any phone number, resulting in unauthorized access to existing WordPress accounts or creation of new arbitrary accounts.	9.8	More Details
CVE-2026-86184	Lara Dashboard before 1.3.0 contains an authentication bypass vulnerability in the screenshot-login route that allows unauthenticated attackers to authenticate as any user by email when APP_ENV is not production. Attackers can request the GET /screenshot-login/{email} endpoint with a registered email address to receive a fully authenticated session, enabling access to user administration, settings, database contents, and arbitrary code execution through the module installer.	9.8	More Details
CVE-2026-86189	WWBN AVideo contains a path traversal vulnerability in notify.ffmpeg.json.php that allows unauthenticated attackers to write files to arbitrary locations by supplying a caller-chosen path in the avideoRelativePath parameter. Attackers can replay any previously issued ciphertext as a notifyCode token, which is decrypted but never validated, to bypass authentication and write files to the application root and subdirectories.	9.8	More Details
CVE-	SQL Injection vulnerability in oasys sysoa version 1.0 allows a remote attacker to execute arbitrary code via		More

2025-67066	the outtype parameter in the /outaddresspaging path	9.8	Details
CVE-2026-79391	No authentication exists in the MQTT service of Trueview 6.0.23.4. The MQTT broker accepts client connections on TCP port 1883 without requiring authentication, allowing a remote attacker with network access to establish an MQTT session and perform unauthorized publish or subscribe operations.	9.8	More Details
CVE-2026-71624	An issue in esoTalk v.1.0.0g4 allows a remote attacker to execute arbitrary code via the core/models/ETMemberModel.class.php, core/controllers/ETMemberController.class.php, and core/lib/ET.class.php components	9.8	More Details
CVE-2026-75816	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Authentication Bypass to Account Takeover in all versions up to, and including, 3.29.12. This is due to the pre_update_value function lacking any capability or ownership check, and ActionPost::conditions_logic() short-circuiting its current_user_can('edit_post') authorization gate whenever the post ID is non-numeric — such as the string user_1 — allowing unauthenticated form submissions to be routed to arbitrary user records without restriction. This makes it possible for unauthenticated attackers to overwrite any user's registered email address, including an administrator's, and then leverage WordPress's native password-reset flow to fully take over the targeted account.	9.8	More Details
CVE-2026-84325	Improper input validation in DataTransfer in Google Chrome prior to 152.0.7977.75 allowed a remote attacker leveraging social engineering to bypass system access restrictions via a co-installed app. (Chromium security severity: High)	9.8	More Details
CVE-2026-78745	An issue in HiDPT/ Weyon HiDPTAndroid Hi3751V350 Hi3751V352E_DMO allows a remote attacker to execute arbitrary code via the Android Debug Bridge (ADB) daemon (adbd)	9.8	More Details
CVE-2026-75430	PowerJob Worker version 5.1.2 (and likely earlier versions) exposes the /worker/deployContainer HTTP endpoint without authentication on the default transport port. This allows a remote attacker to execute arbitrary code.	9.8	More Details
CVE-2026-31020	In DocsGPT 0.15.0 and below, the application provides a custom prompt feature that allows users to define prompt content used during chatbot interactions. This functionality renders user-supplied prompt data using Jinja templates without input sanitization or sandboxing. An unauthenticated attacker can inject malicious template expressions, leading to a server-side template injection (SSTI) vulnerability that can be exploited to achieve full remote code execution (RCE).	9.8	More Details
CVE-2026-86218	N-central is vulnerable to a pre-auth remote code execution This issue affects N-central: before 2026.3.1.14.	9.8	More Details
CVE-2026-86165	A vulnerability was found in Tenda HG10 300001138. This vulnerability affects the function formURL of the file /boaform/admin/formURL. Performing a manipulation of the argument Keywd/urlFQDN results in buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-44402	Voltronic Power SNMP Web Pro 1.1 contains an unauthenticated remote code execution vulnerability in the upload.cgi firmware update endpoint that allows remote attackers to execute arbitrary commands as root by uploading a crafted tar archive without valid credentials. Attackers can supply a malicious tar archive containing arbitrary executable files that are extracted to a privileged directory and executed as root, achieving full system compromise.	9.8	More Details
CVE-2026-85440	MOOS core-moos through 10.4.0 contains a pre-authentication heap overflow vulnerability in MOOSCommPkt packet handling that allows remote attackers to write arbitrary data by declaring a negative packet length. Attackers can exploit the signed integer check in InflateTo() and negative size conversion in recv() to overflow a four-byte heap buffer during the HandShake phase before authentication.	9.8	More Details
CVE-2026-18658	IBM Operational Decision Manager 9.6.0.0, 9.5.0.0, 8.11.1.0, 8.11.0.1, 8.12.0.1, 9.5.0.1, and 9.0.0.1 is vulnerable to SQL injection. An unauthenticated attacker can execute arbitrary SQL statements and leverage database functionality to write a web shell to the application web root, resulting in remote code execution.	9.8	More Details
CVE-2026-85696	SadTalker contains an OS command injection vulnerability in the video muxing process where uploaded audio filenames are interpolated into ffmpeg commands without proper escaping. Attackers can upload audio files with shell metacharacters in the filename to break out of quoted arguments and execute arbitrary system commands when video generation occurs.	9.8	More Details
CVE-2026-19931	A flaw in libcurl makes it wrongly reuse an HTTP connection setup for a given hostname using Negotiate authentication, when the initial request is done using empty credentials. This can make user B's request get sent over user A's previously authenticated connection.	9.8	More Details
CVE-2026-85146	SmartIT Desktop Manager developed by Lightstar has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can obtain the SSH service account credentials and passwords for the SmartIT Agent directly from the application source code.	9.8	More Details

CVE-2026-85425	MOOS-IvP iSay through 24.8.1 contains a remote code execution vulnerability in the SAY_MOOS variable handler that passes unsanitized text to a shell command. Attackers can publish SAY_MOOS messages containing backticks or command substitution syntax to execute arbitrary commands as the iSay process user.	9.8	More Details
CVE-2026-85438	MOOS-IvP through 24.8.1 contains a buffer overflow vulnerability in StringToIvPFunction() where dimension, piece, and degree counts from encoded BHV_IPF payloads are used as allocation sizes and loop bounds without validation. Attackers can supply crafted payloads with mismatched dimension values to write attacker-controlled doubles past the end of the IvPBox weight array, causing memory corruption and potential code execution.	9.8	More Details
CVE-2026-85437	MOOS-IvP through 24.8.1 contains multiple buffer overflow vulnerabilities in IvP function string decoders that trust attacker-controlled length fields without validation. Attackers can craft malicious encoded strings with mismatched declared and actual field lengths to overflow heap and stack buffers, potentially achieving remote code execution through MOOS variables or alog files.	9.8	More Details
CVE-2026-71377	Command Argument Injection Vulnerability in Cosminexus Component Container. This issue affects Cosminexus Component Container: from 11-70-01 before 11-70-03, from 11-60 before 11-60-03, from 11-50 through 11-50-03, from 11-40 through 11-40-03, from 11-30 through 11-30-08, from 11-20 before 11-20-10, from 11-10 through 11-10-11, from 11-00 through 11-00-12, from 09-87 before 09-87-10, from 09-80 through 09-80-04, from 09-70 before 09-70-28, from 09-50 through 09-50-22, and from 09-00 through 09-00-18.	9.8	More Details
CVE-2026-85181	CAT uses Java String.hashCode as the sole integrity check for session cookies without server-side keying, allowing attackers to forge valid checksums offline. Attackers can set the x-forwarded-for header to bypass IP binding validation and create admin sessions with full configuration access.	9.8	More Details
CVE-2026-85109	A vulnerability was determined in Tenda HG10 300001138. This issue affects the function formLogin of the file /boaform/formLogin of the component Boa Web Server. Executing a manipulation of the argument Username can lead to buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-85154	WWBN AVideo contains an authentication failure vulnerability where the video_id_hash credential is a non-expiring, non-revocable bearer token that grants full administrator session access to the video owner's account. Attackers who obtain a video_id_hash can replay it indefinitely to authenticate as the video owner with full privileges, and the credential remains valid even after the owner changes their password.	9.8	More Details
CVE-2026-19117	Under specific conditions, an attacker can register an attacker-controlled FIDO2 credential against a target account and then authenticate as that user. This issue affects on-premises deployments only.	9.8	More Details
CVE-2026-20279	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20279 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) CWE-284.	9.8	More Details
CVE-2026-20274	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20274 are related to improper resource control issues that are grouped under the Common Weakness Enumeration (CWE) CWE-664.	9.8	More Details
CVE-2026-20212	A vulnerability in the Silicon One integration for Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to execute code with root privileges. This vulnerability exists because TCP ports 43210 and 43211 are accessible in the default Layer 3 (L3) virtual routing and forwarding (VRF). A successful exploit could allow the attacker to connect to an affected device and send crafted input that could be executed as code with root privileges. The exploitation of this vulnerability could also cause the S1HAL process to crash, which could cause the device to reload.	9.8	More Details
CVE-2026-53611	Looking Glass is a modern, stateless network-diagnostic platform — a single self-contained Go binary that fronts a fleet of routers over SSH and exposes ping / traceroute / BGP lookups through a gRPC (ConnectRPC) API, an embedded SvelteKit web UI, and a lg-cli client. Prior to version 1.3.5, there is an OS Command Injection vulnerability resulting from an unanchored regular expression in the input validation layer. This issue has been patched in version 1.3.5.	9.8	More Details
CVE-2025-9314	The Developer Tools WordPress plugin through 1.1.3 contains an unauthenticated arbitrary file upload vulnerability in the bundled SWFUpload component	9.8	More Details
CVE-2026-84795	Craft CMS before 5.10.11 fails to validate the admin flag during user registration, allowing it to persist from deactivated admin accounts. Attackers can register with a deactivated admin's email address to inherit administrator privileges when public registration and disabled email verification are configured.	9.8	More Details

CVE-2026-81294	Unauthenticated Privilege Escalation in Authorizer <= 3.15.1 versions.	9.8	More Details
CVE-2026-12744	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote unauthenticated attacker to execute arbitrary code on the server.	9.8	More Details
CVE-2026-78657	The SigmaForms Pro – AI Generated Forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_submission_files function in all versions up to, and including, 1.4.11. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The malicious path traversal URL is submitted via form upload field and stored in the database, with deletion triggered when an administrator deletes the submission record from the admin panel.	9.8	More Details
CVE-2026-9055	The Booking for Appointments and Events Calendar – Amelia (Premium) plugin for WordPress is vulnerable to Privilege Escalation in versions 8.0 - 9.6.2. This is due to insufficient validation of the attacker-controlled 'type' parameter in the customer update endpoint, which allows customers to set their role to 'manager' and trigger creation of a WordPress user with the wpamelia-manager role when the 'externalId' parameter is set to 0. This makes it possible for unauthenticated attackers to escalate their privileges to administrator by first elevating to the manager role, then creating a provider entity linked to an administrator user ID and overwriting that administrator's password.	9.8	More Details
CVE-2026-12745	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote unauthenticated attacker to execute arbitrary code on the server.	9.8	More Details
CVE-2026-61516	Netis NX10 firmware V4.0.1.5808 and V3.0.0.4142 contain an information disclosure vulnerability that allows unauthenticated attackers to retrieve the administrator password by sending a request to the sysinfo action in the web management interface without a valid session. Attackers can replay the exposed credential against the login handler to establish a fully authenticated administrator session on the device.	9.8	More Details
CVE-2026-79576	An issue in the Single-Sign On (SSO) component of Digital-Infrastructure v9.6.7 allows attackers to authenticate as any user, including the Admin, without a password.	9.8	More Details
CVE-2026-79569	Movie_Recommend v1.0.0 was discovered to contain a SQL injection vulnerability in the sort parameter at /loadingmore. This vulnerability allows attackers to access sensitive database information via a crafted SQL statement.	9.8	More Details
CVE-2026-84238	Unauthenticated Broken Access Control in YITH Request a Quote for WooCommerce Premium < 4.46.0 versions.	9.8	More Details
CVE-2026-84753	Unauthenticated PHP Object Injection in Mail Mint <= 1.31.0 versions.	9.8	More Details
CVE-2026-71376	OS command injection vulnerability in Cosminexus Component Container. This issue affects Cosminexus Component Container: from 11-70-01 before 11-70-03, from 11-60 before 11-60-03, from 11-50 through 11-50-03, from 11-40 through 11-40-03, from 11-30 through 11-30-08, from 11-20 before 11-20-10, from 11-10 through 11-10-11, from 11-00 before 11-00-13, from 09-87 before 09-87-10, from 09-80 before 09-80-05, from 09-70 before 09-70-28, from 09-50 through 09-50-22, and from 09-00 through 09-00-18.	9.8	More Details
CVE-2026-86478	In JetBrains YouTrack before 2025.3.161254, 2026.1.14042 improper authentication in YouTrack Helpdesk allowed unauthenticated account takeover via a self-asserted email address	9.8	More Details
CVE-2026-76578	A flaw was found in FreeIPA. The self-managed OTP token ACI does not require authentication and does not restrict which attributes may be added alongside the token entry. An unauthenticated LDAP client can exploit this, combined with a related flaw in the underlying directory server's ACI evaluation (tracked separately), to create an arbitrary attacker-controlled Kerberos principal and have it added to the administrators group. This allows a remote, unauthenticated attacker to obtain genuine FreeIPA administrator-group membership and perform administrative operations against the directory and, on SID-enabled deployments, other IdM services.	9.8	More Details
CVE-2026-85433	MOOS essential-moos pShare through 10.0.1 fails to properly authorize PSHARE_CMD messages, allowing any publisher to reconfigure network routes and listeners at runtime. Attackers can send crafted PSHARE_CMD messages with cmd=output or cmd=input parameters to open new listeners on arbitrary addresses and redirect or duplicate bus traffic to attacker-controlled destinations.	9.8	More Details
	A flaw was found in 389 Directory Server. During SASL PLAIN authentication, a stale identity carried in a Cyrus SASL auxiliary property from a prior failed bind attempt can be installed on a connection following a		

CVE-2026-18922	subsequent, unrelated successful bind, regardless of which SASL mechanism completes that second bind. An attacker can send a SASL PLAIN bind as cn=Directory Manager with an incorrect password, then complete a SASL ANONYMOUS bind on the same connection, causing the server to grant Directory Manager authority without any valid credentials. A variant using a valid low-privileged account's own successful bind instead of an anonymous one is also possible.	9.8	More Details
CVE-2026-85428	MOOS core-moos through 10.4.0 contains an authentication bypass vulnerability in the optional MOOSDB HTTP server that allows unauthenticated clients to write variables. Attackers can send HTTP requests with variable names and values to the MOOSDB HTTP server port to modify MOOS variables including actuator and override commands without authentication.	9.8	More Details
CVE-2026-85426	MOOS-IvP uMemWatch through 24.8.1 constructs shell commands from attacker-chosen MOOS client names without sanitization. Attackers can inject shell metacharacters into client names to execute arbitrary commands as the uMemWatch process user through unquoted redirection targets in system calls.	9.8	More Details
CVE-2026-10196	The Mail Mint – Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.31.0 via deserialization of untrusted input in the 'handle_form_submission' function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code on the server. The vulnerability was partially patched in version 1.23.1.	9.8	More Details
CVE-2026-85424	MOOS core-moos through 10.4.0 lacks authentication in the wire protocol, allowing unauthenticated clients to connect with full publish, subscribe, and database clear privileges. Attackers can bypass the compile-time protocol string check and connect with arbitrary client names to execute privileged operations including DB_CLEAR which resets all variables and clears client mail queues.	9.8	More Details
CVE-2026-7861	Deserialization of untrusted data vulnerability in Next4Biz Information Technologies Inc. CSM (Customer Service Management) allows Code Injection. This issue affects CSM (Customer Service Management): through 07092026. NOTE: The vendor is continuing efforts to remediate the vulnerability.	9.8	More Details
CVE-2026-86480	In JetBrains Hub before 2026.2.52442 an unauthenticated attacker could register a trusted service and gain superuser privileges	9.8	More Details
CVE-2026-62645	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). Information is exposed through the web interface that can be used to calculate the current and past session ID numbers. This could allow an attacker to bypass the authentication and gain unauthorized access to the device.	9.8	More Details
CVE-2026-86543	knowns versions before 0.30.0 serve the management API without authentication on all network interfaces by default, with no password required on fresh installations. Attackers can access the unauthenticated /api/tunnel/start endpoint to provision a public tunnel and republish the API at a publicly accessible address.	9.8	More Details
CVE-2026-58240	SAP NetWeaver Message Server does not sufficiently validate the authenticity of internal application server components during registration. An unauthenticated attacker with network access to the affected service could exploit this weakness to register an unauthorized component and potentially perform unauthorized actions within the application environment, resulting in a high impact on the confidentiality, integrity, and availability of the affected system.	9.8	More Details
CVE-2026-85391	Peppermint through 0.5.5 contains a hardcoded JWT signing secret in docker-compose.yml that allows unauthenticated attackers to forge session tokens for any account. Attackers can use the published secret to mint valid tokens for arbitrary user IDs and access protected endpoints without credentials.	9.8	More Details
CVE-2026-82526	R2R through 3.6.6 contains a stacked SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL statements by manipulating the index name parameter in the vector index creation endpoint. The index name is interpolated directly into a CREATE INDEX statement via string formatting without identifier quoting or allowlist validation, enabling arbitrary DDL and DML execution through semicolon-separated statements under the PostgreSQL superuser account.	9.8	More Details
CVE-2026-71374	Deserialization of untrusted data vulnerability in Cosminexus Component Container. This issue affects Cosminexus Component Container: from 11-70-01 before 11-70-03, from 11-60 before 11-60-03, from 11-50 through 11-50-03, from 11-40 through 11-40-03, from 11-30 through 11-30-08, from 11-20 before 11-20-10, from 11-10 through 11-10-11, from 11-00 before 11-00-13, from 09-87 before 09-87-10, from 09-80 before 09-80-05, from 09-70 before 09-70-28, from 09-50 through 09-50-22, and from 09-00 through 09-00-18.	9.8	More Details
CVE-2026-84834	Unauthenticated PHP Object Injection in JobSearch <= 3.2.0 versions.	9.8	More Details
CVE-2026-84814	Subscriber Privilege Escalation in Bricksforge <= 3.1.8.8 versions.	9.8	More Details

CVE-2026-86124	AutoAgent contains an unauthenticated remote code execution vulnerability in the TCP server that binds to all interfaces and executes attacker-supplied commands as root. Attackers can connect to the exposed communication port and execute arbitrary bash commands within the container, gaining access to bind-mounted host workspace directories.	9.8	More Details
CVE-2026-86509	A flaw has been found in D-Link DIR-895L A1_102b07. This impacts the function sendOffer/sendACK of the file udhcpcd/serverpacket.c of the component udhcpcd. This manipulation causes stack-based buffer overflow. The attack can only be done within the local network. The exploit has been published and may be used.	9.6	More Details
CVE-2026-82533	DeepSeek Harness before 0.1.2-alpha.1 contains an authentication bypass vulnerability in its local HTTP control-plane API that allows attackers to gain full agent control by supplying a spoofed Host header, as the server validates only the client-supplied Host header value rather than the actual TCP connection origin. Attackers can exploit this flaw to invoke privileged commands such as commands/execute with danger-full-access permissions, escalate session approval policies to unconfined execution, and retrieve all stored conversations without any credential or API key.	9.6	More Details
CVE-2026-85047	Improper input validation in Transactions Platform in Google Chrome on on iOS prior to 152.0.7977.82 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-84333	Use after free in Dawn in Google Chrome on on Android prior to 152.0.7977.75 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-75925	Improper neutralization of CRLF sequences in IXON VPN Client before version 1.4.7 allows an attacker to execute commands as root or SYSTEM. Configuration values accepted by the local service are written to a file later consumed by a privileged subprocess, without line-ending sequences being neutralized, which allows additional directives to be introduced into that file. The configuration interface accepts changes without authenticating or verifying the origin of the requester. The injected configuration persists on disk across restarts of the client and the operating system, and the VPN connection continues to function normally, so there is no behavioral change visible to the user.	9.6	More Details
CVE-2026-84352	Use after free in WebGL in Google Chrome on on Android prior to 152.0.7977.75 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-84353	Use after free in Shared Tab Groups in Google Chrome on on Android prior to 152.0.7977.75 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-84354	Incorrect authorization in FileSystem in Google Chrome prior to 152.0.7977.75 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-85050	Out of bounds write in WebGL in Google Chrome on on Android prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-85085	The Canva Android App before 2.376.0 allowed an external origin to be loaded in a privileged WebView. A threat actor who controls the page loaded by the user is able to communicate with Canva using the user’s session.	9.6	More Details
CVE-2026-53649	Joro is a web exploitation framework. Prior to version 1.1.1, Joro's default proxy mode exposes a local API on 127.0.0.1:9090 that performs no authentication and applies a wildcard CORS policy. Because plugin uploads use the CORS-safelisted multipart/form-data content type, cross-origin JavaScript on any page the operator visits can reach privileged endpoints - including uploading a native plugin and triggering a restart - directly through the operator's browser, with no preflight or credentials. Since plugins execute on load, this yields unauthenticated remote code execution as the operator's user from a single page visit. This issue has been patched in version 1.1.1.	9.6	More Details
CVE-2026-85042	Use after free in DevTools in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-19274	IBM Observability with Instana (Agent) Build 1.0.303 through 1.0.323 IBM Instana Agent Operator could allow an authenticated Kubernetes tenant to hijack or permanently destroy another tenant's cluster-level RBAC permissions, caused by cluster-scoped RBAC objects being keyed solely by the bare CR name with no namespace disambiguation, allowing a same-named `InstanaAgent` CR in an attacker-controlled namespace to silently overwrite the shared `ClusterRoleBinding` or delete it outright and revoke the victim agent's cluster monitoring access.	9.6	More Details
CVE-2026-	Improper restriction of excessive authentication attempts vulnerability in Bahçelievler Muncipality BiHayat App allows Authentication Bypass. This issue affects BiHayat App: from 2.1.7 through 07092026. NOTE: The	9.4	More Details

6223	vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-85695	FastChat contains an authentication bypass vulnerability in the /register_worker endpoint that allows unauthenticated attackers to register arbitrary worker addresses and perform server-side request forgery. Attackers can register malicious workers under victim model names to intercept user prompts, images, and responses, or probe internal network ports across the worker mesh.	9.4	More Details
CVE-2026-76969	@sap/cds-mtxs NPM library does not perform sufficient checks on certain functionality used in multitenant CAP applications with extensibility enabled. An unauthenticated attacker could send specially crafted requests to obtain sensitive credentials and abuse them to replace or delete tenant data. Successful exploitation can result in a high impact on availability and integrity of the application. There may also be partial impact to the confidentiality of business data.	9.4	More Details
CVE-2026-61410	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Missing Authorization vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to remote execution. This vulnerability is considered critical because it allows an attacker to execute commands remotely on a target system by sending a specially crafted request to the application, bypassing intended restrictions on code execution.Dell recommends customers to upgrade at the earliest opportunity.	9.4	More Details
CVE-2026-80238	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Execution with Unnecessary Privileges vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to Protection mechanism bypass. This vulnerability is considered critical because a low-privileged operator with SSH access to the SCG host can gain root-level access to the host without requiring a password by leveraging the exposed Docker socket. Additionally, an attacker who compromises a service running within the orchestrator container can access the same socket and escape the container boundary to obtain host-level control. Dell recommends that customers upgrade at the earliest opportunity.	9.3	More Details
CVE-2026-80098	Improper verification of cryptographic signature in Copilot Studio allows an unauthorized attacker to elevate privileges over a network.	9.3	More Details
CVE-2026-85183	Taipy configures its socket.io server with wildcard CORS origin and credential flag enabled, allowing any web page to establish credentialed WebSocket connections to victim applications. Attackers can open socket.io sessions from arbitrary domains and invoke state variable modifications and action callbacks without CSRF protection.	9.3	More Details
CVE-2026-84813	Unauthenticated SQL Injection in GeoDirectory <= 2.8.174 versions.	9.3	More Details
CVE-2026-84768	Unauthenticated SQL Injection in VikAppointments Services Booking Calendar <= 1.2.20 versions.	9.3	More Details
CVE-2026-80726	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: WARN and clear role.invalid when creating a child shadow page Explicitly clear role.invalid when deriving a child shadow page's role from its parent to harden against bugs elsewhere in KVM, as violating KVM's invariant that invalid pages are NOT on the list of active MMU pages leads to use-after-free due to __kvm_mmu_prepare_zap_page() using list_add() instead of list_move() when processing an invalid shadow page, i.e. makes a bad situation far worse. Yell loudly if the parent is invalid, as it means KVM has missed a validity check, i.e. KVM is attempting to map memory using an invalid/obsolete root, but continue on as the child is otherwise still a valid shadow page. == BUG: KASAN: slab-use-after-free in __kvm_mmu_get_shadow_page+0x1817/0x1860 [kvm] Write of size 8 at addr ff11000153dd1368 by task repro/853 CPU: 1 UID: 1000 PID: 853 Comm: repro Not tainted 7.2.0-rc2-3aec122bdcaf-next-vm #5 PREEMPT Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 Call Trace: <TASK> dump_stack_lvl+0x4b/0x70 print_report+0x153/0x49c kasan_report+0xbc/0xf0 __kvm_mmu_get_shadow_page+0x1817/0x1860 [kvm] mmu_alloc_root+0x141/0x320 [kvm] kvm_mmu_load+0x612/0x20f0 [kvm] kvm_arch_vcpu_ioctl_run+0x3dd5/0x6150 [kvm] kvm_vcpu_ioctl+0x5e4/0x10d0 [kvm] __x64_sys_ioctl+0x131/0x1b0 do_syscall_64+0x67/0x5f0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> Allocated by task 853: kasan_save_stack+0x20/0x40 kasan_save_track+0x14/0x30 __kasan_slab_alloc+0x5f/0x70 kmem_cache_alloc_noprof+0xfe/0x2e0 __kvm_mmu_topup_memory_cache+0x135/0x530 [kvm] paging64_page_fault+0x318/0x1e30 [kvm] kvm_mmu_do_page_fault+0x21d/0x630 [kvm] kvm_mmu_page_fault+0x18c/0x17b0 [kvm] kvm_arch_vcpu_ioctl_run+0x1f35/0x6150 [kvm] kvm_vcpu_ioctl+0x5e4/0x10d0 [kvm] __x64_sys_ioctl+0x131/0x1b0 do_syscall_64+0x67/0x5f0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 853: kasan_save_stack+0x20/0x40 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 __kasan_slab_free+0x43/0x70 kmem_cache_free+0xe2/0x400 kvm_mmu_commit_zap_page.part.0+0x1e2/0x310 [kvm] kvm_mmu_free_roots+0x283/0x560 [kvm]	9.3	More Details

	kvm_arch_vcpu_ioctl_run+0x33c8/0x6150 [kvm] kvm_vcpu_ioctl+0x5e4/0x10d0 [kvm] __x64_sys_ioctl+0x131/0x1b0 do_syscall_64+0x67/0x5f0 entry_SYSCALL_64_after_hwframe+0x4b/0x53		
CVE-2026-81286	Unauthenticated SQL Injection in WCFM Marketplace <= 3.8.1 versions.	9.3	More Details
CVE-2026-58400	GeoNetwork is a catalog application to manage spatially referenced resources. Prior to versions 4.4.12 and 4.2.17, the Saxon XSLT processor used to render formatters is configured without secure processing (`FEATURE_SECURE_PROCESSING`) and without disabling Java extension functions (`ALLOW_EXTERNAL_FUNCTIONS`). Any stylesheet loaded by GeoNetwork can therefore invoke `java.lang.Runtime.exec()` or `java.lang.ProcessBuilder` directly, achieving arbitrary command execution as the GeoNetwork process user. A user with sufficient privileges to upload a formatter can deliver a `.xsl` file containing Java extension call that execute arbitrary OS commands with the privileges of the GeoNetwork process. The issue is patched in GeoNetwork versions 4.4.12 and 4.2.17.	9.1	More Details
CVE-2026-85394	python-jose through 3.5.0 fails to properly validate asymmetric keys in HMAC initialization, accepting DER-encoded public keys that lack PEM armor or SSH prefixes. Attackers holding the service's public key can forge HS256 tokens that pass verification when algorithms are not explicitly restricted. This is an incomplete fix for CVE-2024-33663.	9.1	More Details
CVE-2026-66786	A flaw was found in submariner. In cert-auth mode, the connection configuration is built using free-form strings from the Custom Resource Definition (CRD) without proper validation. A malicious cluster can exploit this by publishing a CableName that includes newlines and ipsec.conf directives. This allows an attacker to inject arbitrary configuration parameters or execute commands through leftupdown hooks, leading to remote code execution as root on the gateway node.	9.1	More Details
CVE-2026-73475	Incorrect Authorization vulnerability in Drupal Commerce PayPal allows Forceful Browsing. This issue affects Commerce PayPal versions: from 0.0.0 to 1.12.0, from 2.0.0 to 2.1.3.	9.1	More Details
CVE-2026-84699	Team Password Manager before 14.184.308 fails to enforce authentication requirements in the local account password reset flow. Unauthenticated attackers can reset local account passwords and authenticate as those users to gain unauthorized access.	9.1	More Details
CVE-2026-85043	Incomplete cleanup in Network in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to bypass system access restrictions via crafted network traffic. (Chromium security severity: High)	9.1	More Details
CVE-2026-75156	Apache Airflow FAB provider versions 3.7.3 through 3.8.0 do not validate the issuer or audience of Azure AD `id_token`s during OAuth login. Deployments are affected only when the FAB auth manager is configured with Azure AD as an OAuth provider. Because the signing keys are fetched from Microsoft's **multi-tenant** JWKS endpoint, an `id_token` minted in *any* Azure tenant — including one the attacker creates — passes signature verification, and the username and role assignments are then read from that attacker-controlled token. Anyone able to register an Azure tenant can therefore authenticate to the Airflow UI with no prior access to the deployment. The fix for **CVE-2026-59243** was incomplete, and this advisory closes the remaining gap: that fix made the provider verify the `id_token` signature, but did not add issuer or audience checks. Operators who already applied the CVE-2026-59243 fix are **still affected and must upgrade again** — 3.7.3 is the release that shipped that fix, so every version containing it falls inside this affected range. Upgrade to apache-airflow-providers-fab `3.8.1` or later.	9.1	More Details
CVE-2026-52766	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, the {{erasespamedcomments}} wiki action (actions/EraseSpamedCommentsAction.php) accepts a suppr[] array from POST and deletes every wiki page whose tag appears in that array, with no authorization check anywhere in the action body or in the page-deletion path it invokes. Combined with YesWiki's allow-by-default action ACL model, any user who has page write access, which is the default for everyone (default_write_acl='*') on a fresh install can permanently delete arbitrary wiki pages, including the front page, admin pages, and pages owned by other users. This issue has been patched in version 4.6.6.	9.1	More Details
CVE-2026-85224	A vulnerability was determined in D-Link DNS-320 ShareCenter 2.06B01. This affects an unknown part of the file /cgi/file_sharing.cgi of the component File Sharing. Executing a manipulation of the argument fileurl can lead to os command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	9.1	More Details
CVE-2026-86542	knowns before 0.30.0 fails to validate import names in the import routes, allowing unauthenticated attackers to write files outside the imports directory. Attackers can supply traversal sequences in the name parameter to escape the imports directory and overwrite arbitrary files writable by the server process.	9.1	More Details
CVE-2026-85222	A vulnerability has been found in D-Link DNS-340L 1.01B04. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/addon_center.cgi of the component Add-On Center. Such manipulation of the argument f_name/f_url/f_flag/f_login_user 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.	9.1	More Details

CVE-2026-86190	WWBN AVideo contains a broken access control vulnerability in videoViewsInfo endpoints that returns complete user records including password hashes, recovery tokens, and live session identifiers to unauthenticated callers when a hash parameter is provided. Attackers can use the disclosed session identifier to hijack viewer sessions, including administrator accounts, and obtain sensitive personal data for all video viewers.	9.1	More Details
CVE-2026-86148	A security flaw has been discovered in Tenda CP3 27.5.57.101. This vulnerability affects the function SystemAsh of the file Apis/system.c of the component Kylin. The manipulation of the argument AlarmVoiceURL results in os command injection. It is possible to launch the attack remotely.	9.1	More Details
CVE-2026-86149	A weakness has been identified in Tenda CP3 27.5.57.101. This issue affects some unknown processing of the file Net/NetCheckPing.cpp. This manipulation of the argument interface_name/host causes os command injection. The attack can be initiated remotely.	9.1	More Details
CVE-2026-86151	A vulnerability was detected in Tenda CP3 27.5.57.101. The affected element is the function sub_2F77E8 of the file Apis/system.c of the component Network Configuration Management. Performing a manipulation results in os command injection. The attack may be initiated remotely.	9.1	More Details
CVE-2026-81939	A Zip Slip vulnerability in the SonicWall Network Security Manager (NSM) On-Prem file upload and archive processing functionality allows an attacker to extract files outside the intended destination directory using a specially crafted archive.	9.1	More Details
CVE-2026-86153	A vulnerability has been found in Tenda CP3 27.5.57.101. This affects the function CRedirServer::SetRedirectEnable of the file Functions/Redirect.cpp. The manipulation leads to improper privilege management. Remote exploitation of the attack is possible.	9.1	More Details
CVE-2026-78328	A missing authorization vulnerability in the SonicWall Network Security Manager (NSM) On-Prem Management interface allows a lower-privileged Admin user to escalate privileges to SuperAdmin.	9.1	More Details
CVE-2026-78327	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the SonicWall Network Security Manager (NSM) On-Prem Management interface allows an authenticated attacker with SuperAdmin privileges to inject arbitrary commands that are executed on the underlying host, resulting in remote code execution.	9.1	More Details
CVE-2026-75431	PowerJob Server version 5.1.2 (and likely earlier) uses a predictable JWT signing key for HS256-based authentication. This allows a remote attacker to execute arbitrary code.	9.1	More Details
CVE-2026-75160	An issue in X-Serie Gateway Firmware V6_00_05 allows a remote attacker to escalate privileges via the endpoints /cgi-bin/wwwugw.cgi and /cgi-bin/ugwdownload.cgi.	9.1	More Details
CVE-2026-18924	A flaw in libcurl's handling of HTTP/2 Server Push streams, when the parent handle is set to share connections with other handles, can lead to use-after-free in the cleanup process.	9.1	More Details
CVE-2026-85684	marker through 2.0.0 contains a path traversal vulnerability in the FastAPI /marker/upload handler that fails to sanitize the file.filename parameter. Unauthenticated attackers can supply filenames containing directory traversal sequences to write arbitrary files to any location or delete existing files on the system.	9.1	More Details
CVE-2026-85667	xiaobei through 5.5.2 fails to implement authentication or signature validation on webhook endpoints, allowing unauthenticated attackers to inject arbitrary messages into the agent pipeline. Attackers can publish malicious messages via the /webhook_worktool handler and exploit unvalidated media URL fetching to perform server-side request forgery against internal services.	9.1	More Details
CVE-2026-85184	@fastify/middie versions >= 9.1.0 and before 9.3.4 decide whether to run path-scoped middleware by matching against the raw request target, while the Fastify router resolves an absolute-form request target to its path before dispatching. Because the two layers evaluate different strings, a request using an absolute-form target reaches the route handler while the path-scoped middleware, such as authentication or authorization, is skipped. An unauthenticated network attacker can use this to bypass path-based access controls in a Fastify application that relies on middie for those controls. Users should upgrade to @fastify/middie 9.3.4 or later.	9.1	More Details
CVE-2026-80181	Apache Allura's webhooks are vulnerable to Server-Side Request Forgery (SSRF). This issue affects Apache Allura: through 1.20.0. Users are recommended to upgrade to version 1.21.0, which fixes the issue.	9.1	More Details
CVE-2026-85435	MOOS-IvP uFldNodeBroker through 24.8.1 fails to validate the source of TRY_SHORE_HOST messages on the vehicle bus, allowing any publisher to enroll attacker-controlled shore routes. Attackers can publish malicious shore route messages to receive bridged vehicle traffic including sensor data and control information.	9.1	More Details
CVE-	MOOS-IvP uFldShoreBroker through 24.8.1 fails to verify node ping authenticity before creating outbound		More

2026-85434	bridge routes. Attackers can publish NODE_BROKER_PING messages with crafted HostRecord data to redirect bridged variables to attacker-controlled addresses.	9.1	Details
CVE-2026-85430	MOOS essential-moos through 10.0.1 contains an authentication bypass vulnerability in pShare that accepts UDP datagrams from any source and republishes them with the attacker-claimed identity intact. Attackers can send crafted UDP datagrams to pShare input routes to inject messages into the local MOOS community under spoofed identities, or send malformed datagrams to crash the pShare process.	9.1	More Details
CVE-2026-62916	Authentication bypass using an alternate path or channel in Microsoft Entra ID allows an unauthorized attacker to elevate privileges over a network.	9.1	More Details
CVE-2026-84803	SiYuan before v3.8.2 contains a stored cross-site scripting vulnerability in asset serving due to an incomplete extension blocklist that misses script-capable file types. Attackers can upload files with extensions like .xht, .ehtml, .xsl, .xbl, or .rdf that resolve to executable media types and execute JavaScript to steal API tokens and compromise workspaces.	9.0	More Details
CVE-2026-50093	A vulnerability has been identified in Siveillance Control Pro V3.0 (All versions < V3.0.12.2173), Siveillance Control Pro V4.0 (All versions < V4.0.9.2178), Siveillance Control V3.0 (All versions < V3.0.22.2177), Siveillance Control V4.0 (All versions < V4.0.11.2177). A vulnerability in the OIS web module allows an attacker to upload arbitrary files to the server. Successful exploitation of this vulnerability could allow an attacker to gain root access on the host system, potentially leading to a full compromise of the affected OIS environment.	9.0	More Details
CVE-2026-66768	SAP GUI for Java does not correctly enforce the trust level policy for certain functions invoked from a connected backend system. A low-privileged attacker could exploit this weakness by manipulating a connected backend system to trigger affected functionality. This could allow arbitrary command execution on the victim's machine, leading to a high impact on the confidentiality, integrity, and availability of the affected system.	9.0	More Details
CVE-2026-84324	Use after free in Proxy in Google Chrome prior to 152.0.7977.75 allowed a remote attacker to execute arbitrary code outside the sandbox via crafted network traffic. (Chromium security severity: High)	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-48019	Laravel is a web application framework. Prior to versions 12.60.0 and 13.10.0, a CRLF injection vulnerability in Laravel's email validation, in combination with how Symfony Mailer and Symfony Mime handle certain character sequences, may allow an unauthenticated attacker to interfere with outbound email processing in applications that send mail to user-supplied addresses. This issue has been patched in versions 12.60.0 and 13.10.0.	8.9	More Details
CVE-2026-84796	Craft CMS versions before 5.10.11 contain a site scope bypass vulnerability in GraphQL entry mutation resolvers that fail to validate siteId through ArgumentManager::prepareArguments(). Attackers with tokens scoped to one site can read, modify, or delete entries across unauthorized sites by passing siteId directly in mutation arguments.	8.8	More Details
CVE-2026-84764	Unauthenticated Cross Site Request Forgery (CSRF) in Simply Schedule Appointments <= 1.6.12.23 versions.	8.8	More Details
CVE-2026-85540	DreamMaker developed by Interinfo has a SQL Injection vulnerability. Authenticated remote attackers can inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2026-86482	In JetBrains YouTrack before 2026.2.18634 unchecked group membership changes allowed privilege escalation	8.8	More Details
CVE-2026-84770	Unauthenticated Cross Site Request Forgery (CSRF) in Mang Board WP <= 2.3.8 versions.	8.8	More Details
CVE-2026-85623	goose 1.37.0 executes arbitrary commands from recipe stdio extensions and retry.checks without security inspection. Attackers can distribute malicious recipes that execute shell commands as the user running goose, bypassing the recipe security scan which does not inspect extensions or retry configurations.	8.8	More Details
CVE-2026-	The Canva Android App before 2.376.0 did not restrict the headers returned to an external origin running in a	8.8	More

85094	privileged WebView. A threat actor with control of the WebView could access a user's session.		Details
CVE-2026-19633	PostgreSQL Anonymizer contains a vulnerability that allows unprivileged masked users to execute arbitrary code by abusing operators, domain casts, or view subqueries that carry untrusted expressions. When these objects are evaluated in the context of the extension's masking mechanisms, the malicious code can run with elevated privileges. The issue is fixed in PostgreSQL Anonymizer 3.1.4 and later versions	8.8	More Details
CVE-2026-85452	MOOS ui-moos through 50b9c6c contains a buffer overflow vulnerability in ScopeTabPane.cpp and ScopeGrid.cpp where client and variable names are formatted into fixed 1024-byte buffers using sprintf without length validation. Attackers can supply arbitrarily long MOOS identifiers that overflow the buffers when an operator selects process list entries or pokes variables, enabling code execution.	8.8	More Details
CVE-2026-66842	BIG-IP has a vulnerability where an authenticated user of any role may be able to create administrative user accounts through an undisclosed request to Traffic Management User Interface (TMUI). Impact: This vulnerability may allow an authenticated attacker with network access to the BIG-IP management interface to escalate privileges by creating administrative accounts on the BIG-IP system. There is no data plane exposure; this is a control plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2026-86439	knowns versions before 0.30.0 fail to validate filesystem paths in MCP tool arguments, allowing attackers to read, create, overwrite and delete files outside the project directory. Attackers can supply path arguments containing directory traversal sequences to access arbitrary Markdown files accessible to the server process.	8.8	More Details
CVE-2026-81807	The Simple Ajax Chat WordPress plugin before 20260827 does not escape chat message content before rendering it, allowing unauthenticated users to inject arbitrary HTML attributes into the page and run scripts in the browser of anyone viewing the chat, including administrators.	8.8	More Details
CVE-2026-81737	The FAQ Builder AYS WordPress plugin before 1.8.5 does not sanitize or escape content submitted by unauthenticated visitors before storing it and outputting it in an admin area page, and the escaping it does apply is undone by a subsequent decoding step, leading to Stored XSS which will execute in the context of a logged in administrator.	8.8	More Details
CVE-2026-18480	The SureCart WordPress plugin before 4.6.3 does not ensure that the account affected by a customer update is the same account its permission check authorised, allowing users with a subscriber-level account to change another user's email address, including an administrator's, and take over that account via a password reset. It further allows an attacker-controlled customer record to be associated with an arbitrary user, and discloses customer identifiers and email addresses to any authenticated user, which together make the takeover reachable from a subscriber-level account alone.	8.8	More Details
CVE-2026-86166	A vulnerability was determined in Tenda HG10 300001138. This issue affects the function formWanRedirect of the file /boaform/formWanRedirect of the component Boa Web Server. Executing a manipulation of the argument if can lead to buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-85053	Improper resource exposure in CacheStorage in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-85051	Type confusion in Compositing in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-85049	Use after free in Skia in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-62650	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). Server-side authorization checks in the web-based management interface are not properly enforced, allowing role-based access control (RBAC) restrictions to be bypassed through manipulation of request data. This could allow an authenticated, low-privileged remote attacker to escalate privileges to an administrative level.	8.8	More Details
CVE-2026-81772	Unauthenticated PHP Object Injection in Ninja Forms - Layout & Styles <= 3.0.31 versions.	8.8	More Details
CVE-2026-16502	The Live Composer – Free WordPress Website Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.1.18 via deserialization of untrusted input . This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	8.8	More Details

CVE-2026-19116	The User Frontend WordPress plugin before 4.3.11 does not prevent user-supplied field values from being deserialized when a submitted post is reopened in its frontend editing form, allowing authenticated users with subscriber-level access and above to perform PHP Object Injection, which may lead to remote code execution when a suitable gadget chain is present on the site.	8.8	More Details
CVE-2026-84801	Craft CMS versions before 5.10.11 fail to validate admin status in the actionGetPasswordResetUrl endpoint, allowing non-admin users with administrateUsers permission to mint password reset URLs for administrator accounts. Attackers can generate a valid reset URL for any admin user and set a new password via actionSetPassword, which validates only the verification code without checking the caller's session, enabling complete control-panel takeover.	8.8	More Details
CVE-2026-20280	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20280 are related to improper checking or handling of exceptional condition issues that are grouped under the Common Weakness Enumeration (CWE) CWE-703.	8.8	More Details
CVE-2026-84645	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, objects of types marked as storing their configuration in independent top-level configuration files in Jenkins (such as the global configuration and jobs) can appear as nested field values in user-submitted `config.xml` documents and subsequently handle HTTP requests via Stapler, resulting in remote code execution.	8.8	More Details
CVE-2026-14357	The DevKit Pro plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.3.0. This is due to a missing capability check and missing nonce validation in the DPDEV_install_themes_func() function registered on the wp_ajax_DPDEV_install_themes action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install arbitrary theme ZIP packages containing PHP files that are extracted into the web-accessible wp-content/themes/ directory, which may make remote code execution possible.	8.8	More Details
CVE-2026-20278	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20278 are related to improper neutralization issues that are grouped under the Common Weakness Enumeration (CWE) CWE-707.	8.8	More Details
CVE-2026-84648	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the system log viewer does not escape log record metadata (source, level, and timestamp) resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers in control of agent processes.	8.8	More Details
CVE-2026-81769	Incorrect Privilege Assignment vulnerability in LiquidThemes Booking Hub allows Privilege Escalation. This issue affects Booking Hub: from n/a through 1.3.1.	8.8	More Details
CVE-2026-84650	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, transient fields cannot be excluded from deserialization, allowing attackers able to submit configuration updates to specify the values of transient fields that will be deserialized, the impact depending on how those fields are used.	8.8	More Details
CVE-2026-86404	EAP's Artemis deserialization configuration permits deserialization by default. ObjectMessage.getObject() uses ObjectInputStreamWithClassLoader, which implements allow-list/block-list filtering via its checkSecurity()/isTrustedType() method. However, by default both allow-list and block-list are empty. When the allow-list is empty (size == 0), isTrustedType() returns true for ALL classes. This means all classes are deserializable by default.	8.8	More Details
CVE-2026-81283	Subscriber PHP Object Injection in WP User Frontend <= 4.3.10 versions.	8.8	More Details
CVE-2026-85607	Blinko 1.8.7 contains an authorization bypass (IDOR) vulnerability in multiple tRPC procedures (message.list, message.update, message.delete, message.clearAfter in server/routerTrpc/message.ts and conversation.clearMessages in server/routerTrpc/conversation.ts). Although these procedures require authentication, they query the database by caller-supplied conversation or message ID without verifying that the resource belongs to the requesting account. Any authenticated user can therefore read another user's full AI chat history, modify individual message content, and delete or wipe entire conversations by enumerating sequential integer IDs.	8.8	More Details
CVE-2026-52691	** UNSUPPORTED WHEN ASSIGNED ** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Griffin Hive Metastore Module. This issue affects Apache Griffin Hive Metastore Module: all versions. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in TAC Information Services Internal and External Trade Inc. GOLDENHORN ONEIT allows Blind SQL Injection. This		More

18198	issue affects GOLDENHORN ONEIT: before Göbeklitepe.	8.8	Details
CVE-2026-85617	snipe-it versions before 8.6.3 contain an authorization bypass vulnerability in the bulk delete functionality that allows restricted users to soft-delete users outside their authorized scope. Attackers can include unauthorized user IDs in bulk delete requests to bypass instance-level restrictions and modify or disable accounts they should not access.	8.8	More Details
CVE-2026-86427	LibreNMS before 26.8.0 contains an argument injection vulnerability in the graph_title parameter that allows authenticated attackers to inject arbitrary rrdtool arguments by breaking out of double-quote escaping. Attackers can inject DEF and LINE arguments to read RRD files from unauthorized devices, or use newline injection to execute arbitrary rrdtool commands, bypassing per-device authorization checks.	8.8	More Details
CVE-2026-85610	OpenPanel before 2.3.0 fails to properly validate chart formula expressions, allowing authenticated project members with read access to execute arbitrary code by recovering the native JavaScript Function constructor through mathjs matrix objects. Attackers can use the recovered constructor to load Node.js built-ins and execute operating system commands with the privileges of the API process, bypassing organization authorization boundaries.	8.8	More Details
CVE-2026-84668	Jenkins SAML Plugin 4.618.v441a_27fa_46d2 and earlier allows overwriting the SAML identity provider metadata file through Stapler data binding, allowing attackers to replace it with attacker-controlled content and authenticate as any user.	8.8	More Details
CVE-2026-84669	A path traversal vulnerability in Jenkins Allure Plugin 2.35.2 and earlier allows attackers with Item/Read permission on jobs that publish Allure report results to read arbitrary files on the Jenkins controller's file system.	8.8	More Details
CVE-2026-84670	Jenkins Performance Plugin 1015.v09ca_52b_3370e and earlier does not restrict the classes that can be instantiated when deserializing cached performance reports stored in the build directory on the Jenkins controller, allowing attackers with Item/Configure permission to execute arbitrary code on the Jenkins controller.	8.8	More Details
CVE-2026-84671	Jenkins File Parameter Plugin 425.v3fa_801681b_5e and earlier allows writing files to arbitrary locations on the Jenkins controller file system through Stapler data binding, which can lead to remote code execution.	8.8	More Details
CVE-2026-84672	Jenkins Microsoft Entra ID (previously Azure AD) Plugin 710.v0b_ff8e9cc2d2 and earlier grants Entra group permissions using both the group's unique object ID and its display name, allowing attackers who can create an Entra group with a colliding display name to gain the permissions configured for a privileged group.	8.8	More Details
CVE-2026-84673	Jenkins Customizable Header Plugin 295.v2544b_ca_19b_97 and earlier allows overwriting the plugin's appearance configuration through Stapler data binding, allowing attackers to configure a custom SVG icon containing inline JavaScript, resulting in a stored cross-site scripting (XSS) vulnerability.	8.8	More Details
CVE-2026-85604	Grav before 2.0.18 (affected versions <= 2.0.17) contains a remote code execution vulnerability in the Twig sort filter. The sortFunc wrapper in GravExtension.php hardcodes Twig's isSandboxed argument to false, so unlike |map/|filter/|reduce, |sort accepts a plain function name inside the sandbox; the remaining denylist misses spl_autoload, which performs a PHP include. An authenticated user with only page-write rights (admin.pages or api.pages.write) can supply a crafted payload (e.g., via form frontmatter rendered by the Email plugin) that invokes spl_autoload through the sort filter, resulting in arbitrary PHP execution as the web server user.	8.8	More Details
CVE-2026-20275	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20275 are related to incorrect calculation issues that are grouped under the Common Weakness Enumeration (CWE) CWE-682.	8.8	More Details
CVE-2026-14828	Zohocorp ManageEngine Password Manager Pro versions before 13235, PAM360 versions before 8561, and Access Manager Plus versions before 4405 are vulnerable to an authenticated SQL Injection vulnerability.	8.8	More Details
CVE-2026-84647	In Stapler 2107.v8dfcb_e8ed317 and earlier, except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, Stapler does not restrict the types of objects that can be instantiated via form data binding to those compatible with the expected field type, allowing attackers with Overall/Read permission to instantiate types related to configuration for which that field type was not intended.	8.8	More Details
CVE-2025-9049	The Nokri – Job Board WordPress Theme theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'nokri_account_member_permissions' function in all versions up to, and including, 1.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add new Subscriber users with employer account member permissions, who in turn can escalate privileges by updating the email address of any user, including Administrator users.	8.8	More Details

CVE-2026-84649	In Stapler 1839.ved17667b_a_eb_5 through 2107.v8dfcb_e8ed317 (both inclusive), except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.447 through 2.579 (both inclusive), LTS 2.452.1 through 2.568.2 (both inclusive), an HTTP endpoint serving dynamically generated JavaScript resources embeds the user's cross-site request forgery (CSRF) token (crumb) as a string literal, allowing attackers with control over a page hosted on the same site as Jenkins to obtain a valid crumb for the targeted user's session and perform actions on their behalf.	8.8	More Details
CVE-2026-19887	The Welcart e-Commerce plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.12.1 via deserialization of untrusted input in the Telecom EDY payment callback (usces_action_acting_transaction). Unauthenticated attackers can store arbitrary 'reserve' key/value pairs as order metadata during a public checkout, then invoke the callback with an attacker-chosen 'option' parameter to select and unserialize that metadata without any provider signature, source-address, transaction-identity or ownership check. A POP chain is present in the TCPDF library bundled with the plugin itself, so no additional plugin or theme is required. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, including wp-config.php, which can lead to remote code execution when an attacker re-runs the WordPress installer against a database they control. Successful exploitation is contingent on an admin printing an invoice to trigger file deletion.	8.8	More Details
CVE-2026-84752	Contributor PHP Object Injection in RTMKit <= 2.1.5 versions.	8.8	More Details
CVE-2026-85176	DbGate fails to validate jslid parameters in the jsldata controller, allowing authenticated users to read and write arbitrary files via file:// scheme resolution. Attackers can exploit getJslFileName() to bypass directory containment and access sensitive files including encrypted database credentials stored in connections configuration.	8.8	More Details
CVE-2026-84350	Use after free in TabStrip in Google Chrome prior to 152.0.7977.75 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via UI Interaction. (Chromium security severity: Low)	8.8	More Details
CVE-2026-12648	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.	8.8	More Details
CVE-2026-12651	A Deserialization of Untrusted Data vulnerability in Ivanti Neurons for ITSM before 2026.2 allows a remote authenticated attacker to execute arbitrary code on the server.	8.8	More Details
CVE-2026-18851	Missing authorization in Ivanti Endpoint Manager Mobile before version 12.10.0.0, 12.9.0.2, and 12.8.0.4 allows a remote authenticated attacker to escalate their privileges to admin.	8.8	More Details
CVE-2026-75169	An arbitrary file upload vulnerability in /cgi-bin/ugwupload.cgi of MBS-Solutions X-Serie Gateway firmware V6_00_05 allows a remote authenticated user with Admin role to upload files with arbitrary content to hardcoded paths.	8.8	More Details
CVE-2026-71963	Hermes Agent 0.18.2 through 0.21.0, fixed in commit f6234d0, contains a remote code execution vulnerability that allows attackers to execute arbitrary OS commands by supplying a malicious repository with a crafted .git/config that sets core.fsmonitor to an attacker-controlled command. When a user opens the malicious repository and sends any message, the agent triggers a git status index refresh which executes the injected command in the user's process context, exposing the full environment including configured provider API keys.	8.8	More Details
CVE-2026-52775	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, YesWiki through the latest development branch contains a SQL injection vulnerability in ReactionManager::deleteUserReaction() that allows any authenticated user to inject arbitrary SQL via the {idreaction} and {id} URL path parameters. The parameters are concatenated directly into a SQL LIKE clause without escaping or parameterization. This issue has been patched in version 4.6.6.	8.8	More Details
CVE-2026-85110	A vulnerability was identified in Tenda HG10 300001138. Impacted is the function formWlanSetup of the file /boaform/formWlanSetup of the component Boa Web Server. The manipulation of the argument ssid leads to buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-77826	The RegistrationMagic WordPress plugin before 6.0.9.9 does not verify which application a Facebook access token was issued to before accepting it as proof of identity, allowing unauthenticated attackers to log in as an existing user whose token they can obtain, or to create and log into a new account even when user registration is disabled.	8.8	More Details
CVE-2026-	Craft CMS versions before 5.10.12 contain a remote code execution vulnerability in the element-index endpoint that allows authenticated content editors to instantiate arbitrary classes through the criteria parameter. Attackers can inject a malicious class via criteria[withTransforms][0][class] that reaches		More

86732	ImageTransforms::normalizeTransform(), then use a PHP gadget chain with yii\rbac\PhpManager to execute code by pointing itemFile to a request log containing PHP payload in the User-Agent header.	8.8	Details
CVE-2026-86712	SiYuan before 3.8.2 trusts the attacker-writable text/siyuan clipboard MIME type and skips sanitization in the paste handler, allowing code execution in the Node-enabled desktop renderer. Attackers can craft malicious web pages that write to the clipboard, and when pasted into SiYuan, injected scripts execute with full Node.js access through the Electron main process.	8.8	More Details
CVE-2026-86730	Craft CMS versions before 5.10.12 fail to properly cleanse string-typed field-layout elements, allowing authenticated control-panel users to inject Yii2 behavior attachments and event handlers. Attackers can post field-layout tab elements as JSON strings to bypass cleanse validation, then trigger arbitrary object instantiation and code execution through Craft::createObject().	8.8	More Details
CVE-2026-75161	An issue in the ugw-restart method of /cgi-bin/wwwugw.cgi in MBS-Solutions X-Serie Gateway firmware V6_00_05 allows a remote authenticated user with the low-privileged Standard role to inject arbitrary code into the dpcheck system utility executed as root.	8.8	More Details
CVE-2026-81543	The Abandoned Cart Pro for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 10.7.1. This is due to missing capability checks and nonce verification on multiple AJAX actions including wcap_save_connector_settings, wcap_send_manual_email, wcap_abandoned_cart_info, and wcap_change_manual_email_data. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify SMTP connector settings to route administrator recovery emails through an attacker-controlled server and intercept auto-login links to gain full administrative access. The plugin's auto-login feature must be enabled, which is the default configuration.	8.8	More Details
CVE-2026-84715	FeatherPanel versions before 1.3.7.10 fail to validate permissions in the SubuserController updateSubuser handler, allowing authenticated subusers to modify their own permission records. A subuser with minimal permissions can send a crafted request to grant themselves full server control, enabling unauthorized access to sensitive data, backups, and server configuration.	8.8	More Details
CVE-2026-84347	Use after free in WebRTC in Google Chrome prior to 152.0.7977.75 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-79423	An authenticated remote code execution (RCE) vulnerability in the admin_config.php component of seacms v13.6 allows attackers to execute arbitrary code via a crafted POST request.	8.8	More Details
CVE-2026-85046	Type confusion in V8 in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-84326	Uninitialized resource in V8 in Google Chrome prior to 152.0.7977.75 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-86177	Pterodactyl Panel before 1.14.1 fails to validate action-specific permissions in scheduled task creation, allowing subusers with only schedule.update permission to execute arbitrary console commands. Attackers can create and immediately trigger scheduled tasks that run game-server console commands, control server power state, or create backups without proper authorization checks.	8.8	More Details
CVE-2026-86169	Axolotl through 0.18.0 contains a remote code execution vulnerability in the multipack patch path where trust_remote_code defaults to None instead of False, causing the security guard to be bypassed. Attackers can execute arbitrary Python code by crafting a malicious Hugging Face model repository selected as base_model, which is loaded with hardcoded trust_remote_code=True during AutoModelForCausalLM.from_pretrained.	8.8	More Details
CVE-2026-82538	ILIAS before versions 9.22, 10.10, and 11.3 contains a SQL injection vulnerability in the repository trash table where the table navigation sort field from HTTP requests is passed directly into the ORDER BY clause of a SQL query without validation against declared sortable columns. Authenticated users with write permission on any container can inject arbitrary SQL through the sort parameter, and because multi-statement execution is enabled in the database layer, stacked queries enable full database read and write access as well as administrator account takeover.	8.8	More Details
CVE-2026-77393	In Ignition 8.1.53 and earlier, the Gateway "Create Project Role(s)" setting shipped blank, which permitted any authenticated user to create projects (if they can execute gateway scripts). Ignition 8.1.54 restricts project creation to Designer sessions and no longer relies on this setting. The 8.3 series is not affected.	8.8	More Details
CVE-2026-18486	IBM ContextForge MCP Gateway <= v1.0.7 MCP Context Forge could allow a remote authenticated attacker to obtain sensitive credentials and escalate privileges due to improper validation of jq filters.	8.8	More Details

CVE-2026-80734	In the Linux kernel, the following vulnerability has been resolved: btrfs: initialize inode mapping flags for cached inodes [BUG] When running generic/795 with 8K block size, 4K page size, the test always fails, triggering some ASSERT()s related to folio size: 795 (241074): drop_caches: 3 assertion failed: IS_ALIGNED(start, blocksize) && IS_ALIGNED(end + 1, blocksize), in extent_io.c:1404 (blocksize=8192 root=262 ino=258 start=16826368 end=16830463 mapping min order=0) ----------[cut here]---------- kernel BUG at extent_io.c:1404! Oops: invalid opcode: 0000 [#1] SMP CPU: 8 UID: 0 PID: 241105 Comm: fsstress Tainted: G OE 7.2.0-rc5-custom+ #442 PREEMPT(full) f4bfb352566f3949f29c233ce6f735050a03b245 Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022 RIP: 0010:assert_folio_range.cold+0x3d/0x3f [btrfs] Call Trace: <TASK> btrfs_read_folio+0x9e/0x170 [btrfs 4cd1dd93b341b8ef766643f9512f4a86259567a3] prepare_one_folio.constprop.0+0x104/0x2a0 [btrfs 4cd1dd93b341b8ef766643f9512f4a86259567a3] btrfs_buffered_write+0x285/0xa50 [btrfs 4cd1dd93b341b8ef766643f9512f4a86259567a3] btrfs_do_write_iter+0x1aa/0x210 [btrfs 4cd1dd93b341b8ef766643f9512f4a86259567a3] iter_file_splice_write+0x31a/0x540 direct_splice_actor+0x53/0x170 splice_direct_to_actor+0xe9/0x240 do_splice_direct+0x76/0xb0 vfs_copy_file_range+0x1fd/0x630 __x64_sys_copy_file_range+0xf9/0x220 do_syscall_64+0xe1/0x790 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> ---[end trace 0000000000000000]--- The ASSERT() itself is added by a later patch. The crash is triggered with that new debug patch, and without this fix. [CAUSE] In the above case, the start 16826368 is properly 8K aligned, but the end (16830463 + 1) is not 8K aligned. Furthermore the mapping's minimal folio order is 0, not the expected 1 for 8K block size with 4K page size. So this means some inodes do not have btrfs_set_inode_mapping_order() called on it. The missing btrfs_set_inode_mapping_order() call happens for cached inodes, through the following events: - btrfs_create_new_inode() called for inode X Which properly sets minimal folio order for the VFS inode. - btrfs_update_inode() called for inode X Which calls btrfs_delayed_update_inode() to create a delayed_node into root->delayed_nodes xarray. - Drop cache/memory pressure, evicting in-memory inode X Which evicted the inode X, but delayed_node is still in root->delayed_nodes for future reuse. - btrfs_iget() for inode X called again btrfs_iget() |- btrfs_iget_locked() | |- iget5_locked_rcu() | Which creates a new vfs_inode for btrfs, whose mapping still | has the minimal order as 0. | |- btrfs_read_locked_inode() |- btrfs_fill_inode() | |- btrfs_get_delayed_node() | Which found out the previous node, and use that delayed | node to initialize the new inode. | |- filled = true; |- if (filled) goto cache_index; Which skips the btrfs_update_inode_mapping_flags() and btrfs_set_inode_mapping_order() calls. So the inode still has minimal folio order set as 0, not the required 1. Thus later page cache read will get a folio whose size is smaller than block size, as the mapping has its minimal folio order set as 0 not 1, then trigger the ASSERT(). [FIX] Move the btrfs_update_inode_mapping_flags() and btrfs_set_inode_mapping_order() calls under cache_index label, so that the mapping flags and minimal folio order is always set no matter if we have a cached inode.	8.8	More Details
CVE-2026-19298	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote authenticated attacker to execute arbitrary code due to an authorization bypass in the flow build process.	8.8	More Details
CVE-2026-82712	Tycon Systems TPDIN-Monitor-WEB3 versions 2.2.9 and prior are vulnerable to a cross-site request forgery vulnerability. This could allow an attacker to perform state changing operations on the device.	8.8	More Details
CVE-2026-79376	An issue in the l2cap_handle_data() function of Bestechnic Co., Ltd BES2300 Bluetooth Audio SoC firmware v3.x and earlier allows attackers to cause a Denial of Service (DoS) via sending a crafted L2CAP packet.	8.8	More Details
CVE-2026-85174	SiYuan before v3.8.2 logs API tokens from query parameters in plaintext to an accessible log file when full-text search requests exceed timing thresholds. Authenticated attackers can read the log file via the getFile endpoint to recover admin API tokens and gain permanent administrative access.	8.8	More Details
CVE-2026-85175	SiYuan versions <= 3.8.1 (fixed in v3.8.2) contain an incomplete blocklist in the IsForbiddenAbsPath() function (kernel/util/path_guard.go), which only blocks conf/conf.json by exact match and does not restrict the TLS private key (conf/key.pem) or CA private key (conf/ca.key) stored in the same conf/ directory. Because the getFile handler skips the blocklist for RoleAdministrator and all authenticated users receive RoleAdministrator in v3.8.1, any user (or any client on a default no-auth-code instance) can retrieve these private keys via POST /api/file/getFile. On deployments with TLS enabled, this allows decryption of captured HTTPS traffic (key.pem) and forging of certificates trusted by clients that imported SiYuan's CA (ca.key).	8.8	More Details
CVE-2026-84694	Coolify before 4.2.0 fails to properly escape environment variable key names in Docker commands executed over SSH on managed servers. Authenticated attackers can inject shell metacharacters into environment variable keys to execute arbitrary commands on the server host outside containers.	8.8	More Details
CVE-2026-80465	A vulnerability has been identified in Mendix SAML (Mendix 10 compatible) (All versions < V4.2.3), Mendix SAML (Mendix 11 compatible) (All versions < V4.2.3), Mendix SAML (Mendix 9.24 compatible) (All versions < V3.6.27). Affected versions of the module do not properly validate the SAML response signature. This could allow unauthenticated remote attackers to hijack an account (session) in specific SSO configurations.	8.7	More Details
CVE-2026-	Snipe-IT versions before 8.7.0 contain a CSS injection vulnerability in the Custom CSS field due to incomplete sanitization that reverses HTML encoding on greater-than and double-quote characters. Superusers can plant malicious CSS payloads using @import and url() references to exfiltrate CSRF tokens from other superusers	8.7	More Details

86738	via attribute-selector rules, enabling account takeover.		
CVE-2026-71404	A flaw was found in Rancher Manager. The GlobalRole controller derived the target ClusterRole name from the user-settable `authz.management.cattle.io/cr-name` annotation and overwrote that object's rules without verifying ownership. A user with delegated GlobalRole create or update permission could point the annotation at any existing ClusterRole, such as `cluster-admin`, and revoke the permissions of every principal bound to it. The change persists after the malicious GlobalRole is deleted. This issue affects Rancher: before 2.15.1.	8.7	More Details
CVE-2026-79679	Use of Weak Credentials vulnerability in B&R Industrial Automation GmbH mapp Audit used in mapp Services. This issue affects mapp Audit used in mapp Services: before 6.8.0.	8.7	More Details
CVE-2026-80219	A flaw was found in hawtio-operator. When deploying Hawtio in cluster mode, the operator creates a cluster-scoped OAuthClient with automatic grant approval (GrantMethod: auto) and no client secret (public client). The redirect URIs are derived from the operator-created Route, whose hostname is tenant-controlled via the Hawtio CR spec.routeHostName field. A malicious tenant can register an arbitrary hostname as a valid OAuth redirect target and, because grants are auto-approved, obtain OpenShift access tokens of any cluster user who visits the crafted authorization URL without any consent prompt.	8.7	More Details
CVE-2026-84695	BookStack before 26.05.4 contains a stored cross-site scripting vulnerability in the drawing upload endpoint that accepts unvalidated base64 content and stores it without content inspection. Attackers with editor permissions can upload SVG files containing scripts that execute in administrator browsers when accessed through the image gallery API without content-type validation or CSP headers.	8.7	More Details
CVE-2026-85781	Unverified ownership of a storage access point in the volume deletion component of the Amazon EFS CSI Driver before v3.4.1 might allow an authenticated Kubernetes user with PersistentVolume creation privileges to cause recursive deletion of directories on an EFS filesystem they are not authorized to access, via a crafted PersistentVolume volumeHandle that pairs an access point from one filesystem with a different target filesystem. To remediate this issue, users should upgrade to version v3.4.1.	8.7	More Details
CVE-2026-86123	SQL Chat contains four unauthenticated API endpoints that accept client-supplied database connection parameters and execute arbitrary SQL queries against attacker-specified hosts. Attackers can connect to internal databases, execute SQL commands, enumerate schemas, and pivot into the server's network without authentication.	8.7	More Details
CVE-2026-0799	In BPF instructions that load/store a value from/to a scratch memory register the register index is an unsigned 32-bit integer and must not exceed 15, but libpcap BPF interpreter does not validate the value. In particular uncommon use cases a crafted filter program can cause the interpreter to try reading and writing the OS process memory in the 16GiB starting at the current stack frame on 64-bit architectures and in the entire address space on 32-bit architectures.	8.7	More Details
CVE-2026-20276	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20276 are related to insufficient control flow management issues that are grouped under the Common Weakness Enumeration (CWE) CWE-691.	8.6	More Details
CVE-2026-85614	OpenPanel before 2.3.0 contains an unauthenticated server-side request forgery vulnerability in the GET /tools/site-checker endpoint that accepts a fully client-controlled URL parameter with no private IP filtering or DNS-rebinding protection. Attackers can make the OpenPanel server issue requests to internal services, localhost, and cloud metadata endpoints, reading internal HTTP response titles, headers, status codes, and SSL certificate information.	8.6	More Details
CVE-2024-35585	Oxford Nanopore MinKNOW before 24.06 relies on a client's source IP address for authentication.	8.6	More Details
CVE-2026-86119	Webstudio through 0.296.0 contains an unauthenticated server-side request forgery vulnerability in the /cgi/image, /cgi/video, and /cgi/asset proxy routes when RESIZE_ORIGIN environment variable is unset. Attackers can supply arbitrary URLs to these endpoints to read cloud instance metadata, access internal services, and perform network reconnaissance on the instance infrastructure.	8.6	More Details
CVE-2026-73315	XenForo before 2.3.13 contains a server-side request forgery vulnerability in the PayPal REST webhook handler that allows unauthenticated attackers to cause the server to make outbound HTTP requests to arbitrary destinations by supplying a crafted certificate URL in webhook headers without scheme, hostname, or allowlist validation. Attackers can submit a crafted POST to the PayPal webhook callback endpoint to reach internal network resources including cloud instance metadata services, potentially disclosing IAM credentials or enabling secondary internal service exploitation.	8.6	More Details
CVE-2026-	GeoNetwork is a catalog application to manage spatially referenced resources. Prior to versions 4.4.12 and 4.2.17, the API endpoint for creating a new formatter via file upload is unprotected and allows the upload of external uncontrolled files. An unauthenticated attacker can upload arbitrary `.xsl` or `.zip` formatter files to the server. An unauthenticated attacker can write arbitrary files into the GeoNetwork formatter directory. On	8.6	More Details

63219	its own this constitutes unauthorized write access to server storage. The issue is patched in GeoNetwork versions 4.4.12 and 4.2.17.		
CVE-2026-67367	A vulnerability has been identified in SIMOVE Fleetmanager V3.1 (All versions < V3.1.13), SIMOVE Fleetmanager V3.2 (All versions < V3.2.4), SIMOVE Fleetmanager V3.3 (All versions < V3.3.2), SIMOVE Fleetmanager V4.0 (All versions < V4.0.1), SIPLANT V1.7 (All versions), SIPLANT V2.2 (All versions), SIPLANT V3.0 (All versions), SIPLANT V3.1 (All versions < V3.1.4). Affected devices do not properly validate and neutralize directory traversal sequences in the file-serving endpoint of the embedded HTTP server. This could allow an unauthenticated remote attacker to read arbitrary files from the underlying operating system without any credentials, potentially exposing sensitive data such as credential stores, private keys, and configuration secrets.	8.6	More Details
CVE-2026-19305	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote attacker to obtain sensitive information due to server-side request forgery.	8.6	More Details
CVE-2026-85620	Postgres MCP Pro 0.3.0 contains a restricted-mode bypass vulnerability where function-name validation is not applied to RangeFunction nodes in FROM clauses. Attackers can execute file-reading functions like pg_read_file through FROM-clause syntax to read arbitrary files despite restricted-mode protections.	8.6	More Details
CVE-2026-82304	The Music Store WordPress plugin before 1.4.5 does not sanitise and escape user input before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users.	8.6	More Details
CVE-2026-84700	PikiwiDB (Pika) v3.5.7 exposes an internal protobuf replication server on a port derived from the client port plus 2000 (e.g. 11221 when the default client port 9221 is used) that does not authenticate incoming requests. Although requirepass is intended to gate replication — a slave presents it as masterauth inside its MetaSync request — only the MetaSync handler (HandleMetaSyncRequest) validates it; the frame dispatcher (DealMessage) does not require a completed or attempted MetaSync before routing other message types to their handlers. As a result, an unauthenticated remote attacker can connect directly to the replication port and issue TrySync, DBSync, BinlogSync, and RemoveSlaveNode requests, obtaining the full-sync snapshot and live write stream and removing replica nodes, even when requirepass is configured.	8.6	More Details
CVE-2026-70178	Missing authorization in Microsoft Fabric allows an authorized attacker to elevate privileges over a network.	8.5	More Details
CVE-2026-85651	Trigger.dev versions before 4.5.2 fail to validate environment membership during run replay operations, allowing authenticated attackers to inject task runs into arbitrary environments. Attackers can replay their own runs into other organizations' or projects' environments to consume victim resources and pollute run history.	8.5	More Details
CVE-2026-85616	Snipe-IT versions before 8.6.2 contain an authorization bypass vulnerability in checkout-acceptance report actions when Full Multiple Company Support is enabled. Authenticated users with reports.view permission can enumerate sequential acceptance IDs and soft-delete or trigger reminder emails for acceptances belonging to other companies by exploiting a null check on the legacy users.company_id column.	8.5	More Details
CVE-2026-76958	SAP Integration Suite does not sufficiently validate XML documents accepted from untrusted sources in certain internal components. An attacker with low privileges could submit specially crafted XML payloads containing malicious external entity declarations. Successful exploitation could allow the attacker to read sensitive file contents from the server and expose them through monitoring or logging output, resulting in a high impact on confidentiality. It could also lead to resource exhaustion, causing a low impact on availability. There is no impact on integrity.	8.5	More Details
CVE-2026-65818	Server-side request forgery (ssrf) in Power Automate allows an authorized attacker to elevate privileges over a network.	8.5	More Details
CVE-2026-86492	In JetBrains YouTrack before 2026.2.18634 a shared token cache allowed cross-tenant theft of GitHub App installation tokens	8.5	More Details
CVE-2026-85179	Label Studio through 1.23.0 fails to validate webhook URLs, allowing authenticated users to dispatch requests to internal services including RFC 1918 addresses and cloud metadata endpoints. Attackers can create webhooks targeting private networks and exfiltrate annotation data by enabling payload transmission in outbound requests.	8.5	More Details
CVE-2026-74860	A flaw was found in libxml2 with Python bindings enabled. A remote attacker could exploit this vulnerability by providing a specially crafted XML document containing a Document Type Definition (DTD) with enumerated attribute values. This triggers a double-free error in the SAX attributeDecl callback handler, where a string is freed twice. This flaw can lead to a denial of service (DoS) due to a reproducible crash in Python applications using the libxml2 SAX bindings.	8.5	More Details

CVE-2026-69857	Authorization bypass through user-controlled key in Azure Cosmos DB allows an authorized attacker to perform spoofing over a network.	8.5	More Details
CVE-2026-20502	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11262030; Issue ID: MSV-9196.	8.4	More Details
CVE-2026-20501	In vdec, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11262030; Issue ID: MSV-9197.	8.4	More Details
CVE-2026-80745	In the Linux kernel, the following vulnerability has been resolved: regulator: fp9931: Fix VPOS/VNEG voltage selector table The VPOSNEG_table[] mapping does not match the FP9931 datasheet. The datasheet defines the VPOS/VNEG voltage mapping as: 00h-04h -> 7.04V (-7.04V) 05h -> 7.26V (-7.26V) 06h -> 7.49V (-7.49V) ... 28h-3Fh -> 15.06V (-15.06V) However, VPOSNEG_table[] has two issues: 1. Selector 0x00~0x04 should all map to 7.04V (5 entries), but the table has 6 entries of 7.04V, causing all subsequent entries to be shifted by one position. 2. Selectors 0x29~0x3F should all clamp to 15.06V (23 entries), but the table has only 41 entries. Any selector value above 0x28 would result in an out-of-bounds table access. Fix both issues by removing the duplicate 7.04V entry and appending the missing 23 clamped 15.06V entries, bringing the table to the correct size of 64 entries (0x00~0x3F).	8.4	More Details
CVE-2026-19843	A flaw was found in 389-ds-base. The Cockpit 389 Console's LDAP editor constructs an ldapsearch command by embedding an LDAP entry's distinguished name (DN) into a shell command string without proper escaping. An LDAP user with delegated privileges to create or rename directory entries could craft a malicious DN containing shell metacharacters. When a Cockpit administrator subsequently views the entry in the 389 Console, the embedded shell command executes with root privileges on the directory server host.	8.4	More Details
CVE-2026-80750	In the Linux kernel, the following vulnerability has been resolved: pmdomain: mediatek: fix remaining %pOF after of_node_put() scpsys_get_bus_protection_legacy() looks up several legacy bus protection regmaps from device-tree nodes. Two error paths put the device node before checking whether the regmap lookup failed, but still pass that node to dev_err_probe() with %pOF on failure. If of_node_put() drops the last reference, the later %pOF formatting can dereference a freed device node. Keep the node reference until after the error message has been emitted in the infracfg and SMI lookup paths. Also drop the SMI node before returning when the SMI phandle is missing.	8.4	More Details
CVE-2026-80752	In the Linux kernel, the following vulnerability has been resolved: Input: psxpad-spi - set driver data before use psxpad_spi_suspend() retrieves the controller state with spi_get_drvdata(), but probe never stores it, so suspend dereferences a NULL pointer. Store it during probe.	8.4	More Details
CVE-2026-80753	In the Linux kernel, the following vulnerability has been resolved: ovpn: run deferred work on a module-owned workqueue ovpn queues several work items whose callbacks execute module text. These works currently run on the global system workqueues, so module exit has no driver-owned drain point that guarantees the callbacks have fully returned before the module text can be freed. Object references protect the objects used by the callbacks, but they do not prove that a workqueue function has returned. In particular, a worker can drop the final reference that unblocks device teardown while it is still executing ovpn code. Add a module-owned workqueue and queue all ovpn work items on it. During module exit, unregister rtnl and netlink first, flush the workqueue so ordinary ovpn workers finish, run the final RCU barrier, and destroy the workqueue last. This keeps the workqueue available for cleanup work queued from RCU callbacks, while ensuring no ovpn work item can outlive the module text. The per-device delayed keepalive work remains explicitly disabled during netdev teardown (disable_delayed_work_sync in ndo_uninit), since flush_workqueue does not flush delayed work that is still only pending on its timer.	8.4	More Details
CVE-2025-12737	The administrative operations within the Carbon Console do not adequately validate specific user-supplied input. This oversight allows a malicious actor with administrative privileges to inject and execute arbitrary code remotely. Successful exploitation enables a threat actor with administrative privileges and Carbon Console access to execute remote arbitrary code through specific administrative operations, leading to a complete compromise of the affected system.	8.4	More Details
CVE-2026-86502	In JetBrains IntelliJ IDEA before 2026.2.2 missing TLS and authentication on the IJent gRPC server allowed local code execution on Remote Development hosts	8.4	More Details
CVE-2026-86295	A vulnerability was found in D-Link DIR-895L A1_102b07. This affects the function sendACK of the file udhcpcd/serverpacket.c of the component udhcpcd. The manipulation of the argument Hostname results in command injection. The attack can be executed remotely. The exploit has been made public and could be used.	8.3	More Details
CVE-	YesWiki is a wiki system written in PHP. From version 4.2.0 to before version 4.6.6, ApiController::deletePage() interpolates a page tag retrieved from the database into a DELETE FROM ..._links WHERE to_tag = '$tag' query without escaping. The page tag is attacker-controlled — the POST /api/pages/{tag} API accepts arbitrary URL-encoded values, including single quotes, and stores them. A low-		More

2026-52771	privilege authenticated user can therefore create a page whose tag is a SQL fragment, make the page non-orphaned via the standard {{include page="..."}} link mechanism, and then invoke the delete endpoint to execute arbitrary SQL inside the wiki database - including time-based blind data exfiltration from any table. This issue has been patched in version 4.6.6.	8.3	Details
CVE-2026-85048	Use after free in Compositing in Google Chrome prior to 152.0.7977.82 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-85212	CRMEB contains an authentication bypass vulnerability in the verifyAuth() method of SystemRoleServices.php that returns true from both conditional branches. Sub-administrators and accounts with no roles can access restricted admin endpoints by exploiting the inert role check that always permits requests.	8.3	More Details
CVE-2026-86541	knowns versions before 0.30.0 contain a path traversal vulnerability in the handleCodeReplace() function that allows attackers to overwrite arbitrary files outside the project root. Attackers can supply absolute paths or relative paths containing directory traversal sequences to write malicious content to sensitive files like shell startup scripts or SSH configuration files.	8.3	More Details
CVE-2026-84351	Buffer overflow in GPU in Google Chrome on on Windows prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-84349	Use after free in Browser in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-77180	When NGINX Ingress Controller is configured with Ingress annotations, an injection vulnerability exists in the configuration generator of NGINX Ingress Controller. Multiple user-controllable fields are written into the generated NGINX configuration without sanitization. An authenticated attacker with permission to create or modify these annotations may craft values that inject arbitrary NGINX configuration directives. Impact: An authenticated attacker granted write access to NGINX Ingress Controller Ingress annotations through the Kubernetes API may be able to inject arbitrary NGINX configuration directives, create or delete files, or disable services. There is no data plane exposure; this is a control plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.3	More Details
CVE-2026-52769	YesWiki is a wiki system written in PHP. From version 4.6.2 to before version 4.6.6, the POST /api/forms/{formId}/actor/inbox route - exposed publicly with acl:"public" - accepts an HTTP Signature header whose keyId parameter is a URL. HttpSignatureService::verifySignature() parses the header and immediately makes a server-side HTTP GET to that URL, before any cryptographic verification or URL validation. An unauthenticated remote attacker can therefore make YesWiki issue arbitrary outbound HTTP requests to any host the server can reach - internal services, cloud-metadata endpoints (169.254.169.254), intranet-only admin panels, etc. - and read enough back via timing and error-message oracles to scan ports, enumerate services, and (on a real cloud instance) reach IAM metadata. The only deployment-side precondition is that ActivityPub be enabled on at least one Bazar form. This issue has been patched in version 4.6.6.	8.3	More Details
CVE-2026-82404	TOON is a compact, human-readable serialization of JSON data for LLM prompts. Prior to 2.3.1, decoding attacker-controlled TOON with a __proto__, constructor, or prototype key wrote through the object prototype chain instead of creating an own property, polluting Object.prototype for the runtime. In packages/toon/src/decode/expand.ts, the expandPaths: 'safe' path and insertPathSafe function made dotted keys such as a.__proto__.x the strongest vector, while plain nested objects, tabular rows, quoted keys, and streaming decode were also affected. The encoder also dropped own __proto__ properties and could invoke an inherited setter during normalization. Services that decode untrusted TOON could experience denial of service or, when a suitable downstream gadget is present, remote code execution. This issue is fixed in version 2.3.1.	8.3	More Details
CVE-2026-45730	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.16.0, there is a vulnerability in Nuclio Dashboard's project management API, allowing any authenticated user (without membership in the target project) to bypass OPA authorization checks on write paths (PUT /api/projects/{id}, DELETE /api/projects) and modify or delete any project along with all its associated resources (functions, API gateways, etc.). This issue has been patched in version 1.16.0.	8.3	More Details
CVE-2026-84335	Incorrect authorization in TabStrip in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process and leveraged social engineering to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.3	More Details
CVE-2026-77822	IBM ContextForge MCP Gateway could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery via DNS rebinding.	8.2	More Details
CVE-2026-	OpenPanel before 2.3.0 contains a cross-site scripting vulnerability in the unauthenticated favicon proxy endpoint GET /misc/favicon that allows remote attackers to execute scripts by supplying an SVG file URL. Attackers can host malicious SVG files with embedded scripts that execute in the victim's browser on the API	8.2	More Details

85613	origin, enabling same-origin credentialed requests to authenticated endpoints.		
CVE-2026-52767	YesWiki is a wiki system written in PHP. From version 4.6.2 to before version 4.6.6, HttpSignatureService::verifySignature() checks the result of PHP's openssl_verify() with a loose boolean negation - if (!openssl_verify(...)) { throw ... }. PHP's openssl_verify has four possible return values: 1, 0, -1, and "false". The -1 row is the bypass: PHP's truthiness rules make -1 a truthy value, so !(-1) === false, the throw is skipped, and the controller proceeds to processActivity(). Any condition that makes OpenSSL's EVP_VerifyFinal() return -1 triggers the bypass. The reachable consequence is the controller silently treats a failed verification as success and processes the attacker's payload. This issue has been patched in version 4.6.6.	8.2	More Details
CVE-2026-86145	PCRE2 before 10.48 allows a pcre2_dfa_match out-of-bounds write because reuse of a cached workspace block, in a recursive DFA matching workspace, lacks a size check (even though a newly allocated block, for the same purpose, does have a size check). This outcome requires an attacker-controlled regular expression, or a recursive pattern in conjunction with a small heap limit (this can be set through the API).	8.2	More Details
CVE-2026-84696	Phison PS3111-S11 controller firmware versions through SBFQT1.3 expose privileged vendor unique commands over the ATA interface with absent or defeatable authentication mechanisms. Attackers can bypass the weak CRC-16 based unlock handshake or exploit builds with no VUC lock to read and write controller memory and raw flash, persisting implants across power cycles.	8.2	More Details
CVE-2026-86600	In affected Snowflake drivers, WORKLOAD_IDENTITY authentication requests a cloud workload-identity token and attaches it to the login request without verifying that the configured host is a Snowflake endpoint. An attacker who can modify the connection configuration can cause the driver to mint a fresh attestation and send it to a host they control. The captured token can be replayed to Snowflake for its remaining lifetime in accounts where that workload identity is already registered. On Azure, the token audience is also taken from connection configuration. Combined with an attacker-controlled host, the driver can request a Managed Identity access token scoped to a non-Snowflake Azure resource and deliver it to the attacker. That path is the only case in which impact extends beyond Snowflake; it is bounded by the token lifetime and the managed identity’s permissions. Successful exploitation requires WORKLOAD_IDENTITY authentication on a workload that already has an ambient cloud identity. Patched driver versions restrict this authenticator to recognized Snowflake hosts. Users must manually upgrade.	8.2	More Details
CVE-2026-84757	Unauthenticated Settings Change in WP Compress <= 7.21.28 versions.	8.2	More Details
CVE-2021-38489	HDD password plaintext is stored in a UEFI variable.	8.2	More Details
CVE-2025-15485	The Auto x LINE WordPress plugin through 1.0.0 does not have authorization checks in some of its REST endpoints, allowing unauthenticated users to call them and update the plugin settings, clear logs etc	8.2	More Details
CVE-2026-77968	A flaw was found in hawtio-operator. The operator's ClusterRole grants secrets: [create, get, list, update, watch] across all namespaces. While the operator uses a controller-runtime label-selector cache as a memory optimization, the ServiceAccount token authorizes read access to every Secret in the cluster. The operator also bypasses the cache via direct API calls. Compromise of the operator pod would yield read access to every Secret in the cluster, including bootstrap tokens, cloud credentials, and other operators' secrets.	8.2	More Details
CVE-2026-44506	Medplum is a developer platform that enables development of healthcare apps. In Medplum versions 4.1.10 through 5.1.6, the /oauth2/register endpoint could return the client_secret of preconfigured OAuth clients defined via the defaultOAuthClients server configuration when a matching redirect_uri was provided. This issue has been patched in version 5.1.7.	8.2	More Details
CVE-2026-63376	toml-node is a TOML parser for Node.js and the browser. Prior to 4.1.2, toml.parse() in lib/compiler.js can be tricked by a table path such as a.b.y.__proto__.__proto__, allowing traversal from a scalar value into Number.prototype and Object.prototype. The currentPath tracking value uses both arrays and strings, so valueAssignments records a comma-joined path such as a,b.y while deepRef checks the dot-joined path a.b.y, allowing the duplicate-key guard to miss and attacker-controlled keys to be written to Object.prototype. A table-array prefix-clearing path in addTableArray can also erase guard state before the same __proto__ traversal. Injected properties become visible throughout the Node.js process and can cause denial of service, logic or authorization bypass, or code execution when an application contains a suitable gadget. This issue is fixed in version 4.1.2.	8.2	More Details
CVE-2026-18329	Description NGINX JavaScript (njs) and QuickJS (qjs) engines have a vulnerability when a js_access handler performs asynchronous request body processing and an exception is thrown during asynchronous access-control evaluation before an explicit access denial is returned. An unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request that triggers an error condition in the access validation logic. This may cause the js_access phase to fail open, allowing the request to proceed instead of being denied, resulting in an authentication or authorization bypass and unauthorized access to protected resources.	8.2	More Details

	Impact This vulnerability may allow remote attackers to bypass js_access controls. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
CVE-2026-34223	A vulnerability has been identified in Desigo CC ClickOnce Client V6 (All versions), Desigo CC ClickOnce Client V7 (All versions), Desigo CC family V8 (All versions), Desigo CC family V9 (All versions), Desigo CC Flex Client V6 (All versions), Desigo CC Flex Client V7 (All versions), Desigo CC Installed Client V6 (All versions), Desigo CC Installed Client V7 (All versions). The affected application is vulnerable to Client Code Execution (CCE) due to insufficient input validation when handling scripts embedded within user-defined graphics documents. Specifically, when the script within a graphics document is designed or modified by an attacker to include malicious commands. When a user opens a compromised graphics document, the embedded script is executed on the client application instance, allowing an attacker to write arbitrary files to the client's operating system. Successful exploitation requires an attacker to craft a malicious graphics document and entice a user with sufficient privileges to display it. This could lead to compromise of the client operating system and potential lateral movement within the organization.	8.2	More Details
CVE-2026-85432	MOOS core-moos through 10.4.0 fails to validate client identity in MOOSDB message processing, allowing authenticated attackers to attribute writes to other clients by supplying arbitrary source identifiers in serialized messages. Attackers can forge message origins and cancel third-party subscriptions by exploiting the disconnect between authenticated connection identity and wire-supplied source attribution.	8.2	More Details
CVE-2026-85455	MOOS core-moos through 10.4.0 contains a buffer over-read vulnerability in CMOOSCommPkt where a four-byte packet triggers out-of-bounds memory access during deserialization. Attackers can open a TCP connection to the MOOSDB port and send a crafted short packet to read memory before authentication.	8.2	More Details
CVE-2026-79645	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	8.2	More Details
CVE-2026-20277	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XR Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20277 are related to protection mechanism failure issues that are grouped under the Common Weakness Enumeration (CWE) CWE-693.	8.2	More Details
CVE-2026-82209	When libpsl support is enabled, libcurl fails to enforce the Public Suffix List boundary check when processing a `Set-Cookie` header where the `Domain` attribute explicitly matches an origin host that is itself a public suffix (e.g., `Domain=co.uk` set by `co.uk`). Instead of coercing it into a strict host-only cookie, libcurl saves the cookie with wildcard domain scope (`.co.uk`). Consequently, the cookie is inappropriately included in subsequent outbound requests or HTTP redirects to arbitrary sibling subdomains under the same public suffix (e.g., `attacker.co.uk`).	8.2	More Details
CVE-2026-85160	AVideo through commit c91b5975d contains a cross-site request forgery and path traversal vulnerability in stopLive.php that allows attackers to delete directories by exploiting missing token validation and unsanitized key parameter concatenation. Attackers can craft an image tag with a traversal payload like key=../../videos to trigger recursive deletion of the videos directory when an admin visits a malicious page.	8.1	More Details
CVE-2026-18221	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to gain unauthorized access due to improper validation of client-supplied authentication parameters.	8.1	More Details
CVE-2026-84504	fastify versions before 5.12.2 treat the object resolved by a successful Ajv async validator as the value result protocol used by custom validator compilers. If a request that passes its route schema contains a property named value at the root, fastify replaces the entire request body with that property's value before the handler runs, so the handler receives a different object than the one that satisfied the schema. An authenticated low-privilege caller can use this to make nested data replace the validated body and trigger an operation the route schema did not authorize, leading to unauthorized state changes and data disclosure. Users should upgrade to fastify 5.12.2 or later.	8.1	More Details
CVE-2026-9317	Nango before 0.71.6 contains a missing authentication vulnerability in the runner tRPC server that allows unauthenticated attackers to execute arbitrary JavaScript code by invoking the exposed start procedure without credentials. Attackers with network access to the runner port can send requests to the unauthenticated start procedure, bypassing the unenforced RUNNER_SECRET_KEY environment variable, to achieve remote code execution within the runner process.	8.1	More Details
CVE-2026-18175	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to manipulate database transactions due to improper authorization in the DDM target dispatcher.	8.1	More Details
	Description NGINX JavaScript (njs) has a vulnerability in the XML module's namespace prefix list parser, reachable through the xml.exclusiveC14n() method. An unauthenticated remote attacker can trigger it when an affected NGINX configuration passes an externally controlled XML namespace prefix list to that method.		

CVE-2026-78689	Both the njs and the QuickJS (qjs) engines are affected. A crafted prefix list causes an out-of-bounds write past the end of a heap allocation. With the njs engine, which is the engine used when the js_engine directive is absent, this corrupts adjacent objects and crashes the NGINX worker. With the QuickJS engine, the same call additionally leaks the prefix list on every invocation, causing worker memory to grow across requests. The official nginxinc/nginx-saml reference implementation is affected during SAML signature verification. It reads InclusiveNamespaces/@PrefixList from an untrusted SAML message and passes it to xml.exclusiveC14n() before the signature has been verified, so a valid SAML signature is not required. A crafted SAML Response, Assertion, LogoutRequest, or LogoutResponse is sufficient. Code execution has not been demonstrated and cannot be ruled out for all platforms, as the effect of the out-of-bounds write depends on conditions beyond the attacker's control. Impact This vulnerability allows remote attackers to cause a denial of service on the NGINX system, either through repeatable worker restarts or through worker memory growth or possibly trigger code execution. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-85694	LaVague 0.2.35 contains a remote code execution vulnerability in PythonFromMarkdownExtractor.extract_as_object that evaluates untrusted language model output derived from web page content. Attackers can inject malicious Python code through web pages using indirect prompt injection to execute arbitrary code on the operator's host without review.	8.1	More Details
CVE-2026-66362	Description: When NGINX Plus is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric. User-supplied string values from the Authentication Filter Custom Resource Definition clientID or cookieName fields, or in the clientSecret field of a Secret referenced by an Authentication Filter, are rendered directly into NGINX configuration templates without sanitization or escaping. Impact: An authenticated attacker with permission to create or modify these resources may craft values that inject arbitrary NGINX configuration directives. This is a control plane issue; there is no data plane exposure.	8.1	More Details
CVE-2026-85625	sift (sift.js) 17.1.3 enumerates query keys with for...in, which walks the object prototype chain, and dispatches any matched operator key including $where. The $where operation compiles a string value into a function using new Function unless CSP_ENABLED is set (not set by default). As a result, if a prototype-pollution primitive elsewhere in the process sets Object.prototype.$where to a malicious string, even benign filter calls such as sift({}) execute arbitrary JavaScript. Additionally, passing an untrusted query object containing a string $where directly to sift results in code execution under the default configuration.	8.1	More Details
CVE-2026-85427	MOOS essential-moos pAntler through 10.0.1 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary programs by publishing a crafted MISSION_FILE message to the MOOSDB. Attackers can publish a mission file containing malicious Run entries that pAntler parses and executes via execvp() without authentication validation.	8.1	More Details
CVE-2026-85214	vhr fails to validate user authorization in the PUT /hr/info endpoint, allowing authenticated users to modify arbitrary HR profiles by supplying any profile ID in the request body. Attackers can overwrite other users' names, addresses, and disable accounts including administrators to cause denial of service.	8.1	More Details
CVE-2026-85660	cli-mcp-server 0.2.5 contains a command allowlist bypass vulnerability in the _validate_command_with_operators function when ALLOW_SHELL_OPERATORS is enabled. Attackers can use shell command substitution syntax like $(...) or backticks to execute non-allowlisted commands that bypass the ALLOWED_COMMANDS validation check.	8.1	More Details
CVE-2026-19303	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote authenticated attacker to delete arbitrary local files or directories due to improper limitation of a pathname to a restricted directory.	8.1	More Details
CVE-2026-84779	Subscriber Broken Access Control in Agentimus – AI SEO, llms.txt & MCP for AI Agents <= 1.51.0 versions.	8.1	More Details
CVE-2026-78583	Incorrect Authorization (CWE-863) in Kibana can lead to privilege escalation via Input Data Manipulation (CAPEC-153). Elasticsearch cluster privilege declarations originating from integration packages were not validated before being used to mint credentials for enrolled Elastic Agents. A user holding Fleet management privileges could therefore cause every Elastic Agent on a targeted policy to receive a credential carrying arbitrarily elevated Elasticsearch cluster privileges, up to and including full cluster administration.	8.1	More Details
CVE-2026-82302	Incorrect Authorization (CWE-863) in Kibana can lead to unauthorized configuration modification via Exploiting Incorrectly Configured Access Control Security Levels (CAPEC-180).	8.1	More Details
CVE-2026-85388	Worklenz through 3.0.0 fails to properly validate the sort-field query parameter in pagination helper functions, allowing authenticated users to inject arbitrary PostgreSQL expressions into ORDER BY clauses. Attackers can use time-based and boolean-based blind SQL injection techniques to extract sensitive database content including password hashes from other tenants. This is an incomplete fix for CVE-2026-25947.	8.1	More Details
	HTTPX2 is a next generation HTTP client for Python. Prior to 2.10.0, httpcore2 fails to start TLS in		

CVE-2026-84381	src/httpcore2/httpcore2/_sync/socks_proxy.py and src/httpcore2/httpcore2/_async/socks_proxy.py when the remote origin uses wss through a SOCKS5 proxy because the TLS upgrade condition only recognizes https. HTTPX2 exposes the flaw through Client.websocket() and AsyncClient.websocket() from 2.6.0 through 2.9.1, so the opening handshake, query parameters, Authorization headers, cookies, and subsequent frames can cross the proxy path in plaintext without certificate verification. An attacker controlling or observing that path can read or modify traffic and impersonate the WebSocket server. This issue is fixed in httpcore2 2.10.0 and HTTPX2 2.10.0.	8.1	More Details
CVE-2026-47297	Deserialization of untrusted data in SQL Server allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-82053	A security issue exists in MongoDB's LDAP authorization integration where pooled LDAP connections can retain stale authentication identities after user authentication under certain configurations. Subsequent authorization queries may execute under an unintended LDAP identity rather than the expected one. This can result in incorrect role assignments based on the LDAP directory's access control configuration, potentially allowing an authenticated user to acquire elevated privileges that were not intended by the deployment's authorization policy.	8.1	More Details
CVE-2026-86723	AVideo through c3edcc274c389816d434acadac07ee78eaf330c1 contains an authentication bypass vulnerability in LoginControl::verifyChallenge() that uses loose comparison (==) instead of strict comparison (===) against unset session values. Attackers with only a password can submit an empty request to verifyChallenge.json.php to bypass PGP two-factor authentication and gain full authenticated access.	8.1	More Details
CVE-2026-86722	AVideo through commit c3edcc274c389816d434acadac07ee78eaf330c1 contains an authentication bypass vulnerability where sqlDAL caches empty result sets that writeSql never invalidates. Attackers with a valid password can bypass email two-factor authentication on new devices because the confirmation code hash fails to generate from the stale cached empty result.	8.1	More Details
CVE-2026-84334	Incorrect authorization in Chromoting in Google Chrome on on Windows prior to 152.0.7977.75 allowed a local attacker to execute arbitrary code outside the sandbox via a local program. (Chromium security severity: Medium)	8.1	More Details
CVE-2026-80467	The Advanced Custom Fields: Extended WordPress plugin before 0.9.2.7 does not restrict the role submitted through its front-end user forms to the roles the form actually offers, and its safeguard against privileged roles is incomplete, allowing unauthenticated visitors to register an account with elevated capabilities and then escalate it to administrator.	8.1	More Details
CVE-2026-86297	A vulnerability was identified in D-Link DIR-605 B1v202WWB03. This issue affects the function tunnel_set_params of the file progs.gpl/pppd.alpha/l2tp/tunnel.c of the component L2TP Control Message Parser. Such manipulation of the argument peer_hostname leads to off-by-one. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The exploit is publicly available and might be used.	8.1	More Details
CVE-2026-82061	A use-after-free security issue exists in the server's query execution memory tracking subsystem. An authenticated user with read privileges can trigger a write to freed heap memory through a sequence of standard database commands, leading to server process crash or potential memory corruption. No user interaction is required.	8.1	More Details
CVE-2026-86720	WWBN AVideo through commit c3edcc274c389816d434acadac07ee78eaf330c1 fails to validate ownership of live_restreams_id in resendRestreamer.json.php, allowing authenticated users with canStream to access other users' restream destinations. Attackers can broadcast their live stream to victim-configured restream destinations by supplying arbitrary live_restreams_id values, hijacking YouTube, Facebook, or Twitch streams using victim stream keys.	8.1	More Details
CVE-2026-86544	knowns versions before 0.30.0 contain an authorization bypass vulnerability where mutating code actions are incorrectly classified as read-only operations. Attackers with read-restricted sessions can exploit code.replace to modify permission configurations and escalate privileges on subsequent calls.	8.1	More Details
CVE-2026-79678	A flaw was found in FreeIPA's idp-add command, where insufficiently validated --organization/--base-url input reaches a constrained eval() call before the corresponding LDAP access control check is enforced. This allows any authenticated IPA principal, regardless of privilege level, to enumerate and read the environment variables of the affected server process and to cause denial of service via memory exhaustion.	8.1	More Details
CVE-2026-83527	An Authentication Bypass vulnerability in Sentry before R10.8.2, R10.7.3 and R10.6.4 allows a remote unauthenticated attacker to gain administrative level access.	8.1	More Details
CVE-2026-82684	Tycon Systems TPDIN-Monitor-WEB3 versions 2.2.9 and prior are vulnerable to a Missing Authorization vulnerability. This could allow an attacker to extract system credentials, configurations, or flash contents.	8.1	More Details
CVE-	Improper handling of case sensitivity in the configuration validation component of MongoDB Server may		

2026-82067	cause the authorization subsystem to remain in a default disabled state during server startup. An unauthenticated user with network access to a deployment where this condition occurs can perform arbitrary administrative operations, resulting in full impact of data confidentiality, integrity, and availability.	8.1	More Details
CVE-2026-14982	The WP File Download plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete function in all versions. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The two-stage exploit requires a first request to the file.save task to persist the path-traversal string into file metadata, followed by a second request to the file.delete task to trigger the unlink call — both endpoints lack capability checks and nonce enforcement.	8.1	More Details
CVE-2026-80132	ell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	8.1	More Details
CVE-2026-19219	In Progress® Telerik® UI for AJAX prior to v2026.3.812, insufficient integrity protection of dialog request parameters used by the RadEditor file browser may allow an attacker who has obtained certain application encryption key material to alter the folders the file browser reads from, writes to, and uploads into, potentially resulting in remote code execution.	8.1	More Details
CVE-2026-82071	Insufficient validation of storage engine configuration options in MongoDB Server allows an authenticated user with write privileges to supply crafted parameters during collection creation that override internal storage metadata. This results in an out-of-bounds memory write in the server process, causing a denial of service via server crash, with potential for further impact including arbitrary code execution.	8.1	More Details
CVE-2026-61699	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. Prior to version 0.7.1, revocation is the only in-band mechanism that isolates a compromised/offboarded host from a Nebula mesh. Because the blocklist never reaches any peer's config.yml, a Blocked host retains full overlay reachability to every peer under its CA (and internal services on the mesh) for up to 30d (agent) / 365d (mobile). An attacker who exfiltrates host.key+host.crt can run stock slackhq/nebula directly, ignore the agent's 403/410 poll responses, and stay connected after the operator revokes the host. Operator-visible state (UI shows blocked, audit log records it) is misleading. This issue has been patched in version 0.7.1.	8.1	More Details
CVE-2026-84393	A improper validation of certificate with host mismatch vulnerability in Fortinet FortiOS 7.6.1 through 7.6.6, FortiProxy 7.6.2 through 7.6.6 may allow attacker to information disclosure via <insert attack vector here>	8.1	More Details
CVE-2026-75021	fastify-cli starts the Node.js Inspector when a debug flag is used, but it ignores the explicit bind address the user supplies and binds the Inspector to a broadly reachable address instead of the intended loopback. As a result the debugging interface can be exposed beyond the local machine, and because the Inspector protocol allows arbitrary code evaluation, a remote party that reaches it can achieve remote code execution on the developer's machine. This affects fastify-cli from 1.5.0 up to 8.0.1. Users should upgrade to fastify-cli 8.0.1, which honors the configured Inspector bind address.	8.1	More Details
CVE-2026-86479	In JetBrains YouTrack before 2026.2.18788, 2026.1.14055, 2025.3.161254 missing authorisation allowed access to restricted REST API resources via IDOR	8.1	More Details
CVE-2026-12526	The Advanced Custom Fields: Extended WordPress plugin before 0.9.2.7 does not verify that the requester is authorized to edit the targeted user account in the update-user action of its front-end Forms module; it only checks a capability when the submitted role is administrator or super_admin. On a site that exposes a publicly reachable front-end form whose user-update action targets an existing administrator (a fixed target, or one mapped to a visitor-submitted field) and maps the password to a visitor-submitted field, an unauthenticated visitor can overwrite that administrator's password and take over the account. The default target is the submitting user, so exploitation depends on the form being configured to target another account.	8.1	More Details
CVE-2026-86242	Bifrost HTTP transport before 2.0.0 accepts an enabled custom plugin whose path is an HTTP URL through unauthenticated POST /api/plugins when management authentication is disabled (the default, governance.auth_config.is_enabled=false). The shared-object loader treats an http-prefixed path as a download URL, writes the body to a temporary .so, and passes it to Go's plugin.Open. After a successful open, optional Init runs immediately with the supplied config as the Bifrost process user. On documented dynamically linked builds (DYNAMIC=1 / no static-link flags), which the vendor requires for custom Go plugins, plugin.Open is expected to succeed and this is unauthenticated remote code execution. On the published statically linked Docker image, plugin.Open fails with Dynamic loading not supported, so that build class is only server-side request forgery. Attack complexity is High because the attacker cannot force RCE on the default static image and a loadable plugin must match the host Go version, OS, architecture, and linkage. The 1.6.x HTTP transport line through 1.6.11 does not contain the fix.	8.1	More Details
CVE-2026-	The OAuth Single Sign On WordPress plugin before 7.0.1 does not verify the identity assertion returned by its Steam single sign-on flow, allowing unauthenticated attackers to log in as an arbitrary non-administrator	8.1	More

82183	user, and to create new accounts.		Details
CVE-2026-86117	Coolify through 4.3.17 contains an authentication bypass vulnerability in the OAuth callback handler that signs users into existing accounts based solely on email address without verifying provider assertions or binding OAuth identities. Attackers can register a victim's email address on any enabled OAuth provider to obtain authenticated sessions as that user, bypassing password requirements and two-factor authentication.	8.1	More Details
CVE-2026-85012	Improper neutralization of special elements used in an OS command (CWE-78) in the blueprint resynthesis framework in Amazon Web Services codecatalyst-blueprints before 0.3.156 might allow a user with permission to commit to a repository in the project to execute arbitrary commands in the blueprint resynthesis environment via shell metacharacters in the owner field of a [local] merge strategy entry in a crafted .ownership-file. Version 0.3.156 removes shell interpretation of the owner field, running the command directly rather than through a shell, and rejects values outside an allowlisted command form. This eliminates shell metacharacter command injection. To remediate this issue, users should upgrade to version 0.3.156 or later. No action is required for use of the Amazon CodeCatalyst service. Resynthesis runs in an isolated per-project environment with scoped credentials, and the service applies server-side validation there that rejects [local] merge strategy commands outside a restricted allowlisted form, including for blueprint versions published before 0.3.156.	8.0	More Details
CVE-2026-86185	Bilibili Desktop through 1.18.0 disables TLS certificate verification process-wide and executes unsigned remote JavaScript configuration without integrity checks. An attacker in an on-path network position can intercept configuration fetches, inject arbitrary JavaScript executed in the renderer with access to the privileged IPC bridge, and execute system commands or steal login credentials.	8.0	More Details
CVE-2026-49832	DSpace open source software is a repository application which provides durable access to digital resources. From versions 8.0-rc1 to before 8.4, versions 9.0-rc1 to before 9.3, and version 10-rc1, Remote Code Execution (RCE) is possible via Velocity Templates used by DSpace for COAR Notify/LDN messages. This issue has been patched in versions 8.4, 9.3, and 10.0.	8.0	More Details
CVE-2026-53932	laravel-backup-restore restores database backups made with spatie/laravel-backup. Prior to version 1.9.4, a crafted backup archive can trigger OS command injection during database restore. This issue has been patched in version 1.9.4.	8.0	More Details
CVE-2026-84935	The HT Menu WordPress plugin before 1.2.7 does not perform any capability or object-ownership check when saving navigation menu-item settings, and does not escape those stored settings when the menu is rendered, allowing users with minimal permissions such as Subscribers to store JavaScript that executes in the browser of any visitor, administrators included, who views the affected menu.	8.0	More Details
CVE-2026-84934	The JCH Optimize WordPress plugin before 6.0.1 does not perform a capability check on one of its authenticated AJAX actions and lets the request choose which internal action runs, allowing any authenticated users such as Subscribers to import arbitrary JCH Optimize WordPress plugin before 6.0.1 settings and store a script that executes in the browser of any visitor or administrator viewing the site.	8.0	More Details
CVE-2026-80747	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Add bounds check for CRAT subtype length The CRAT parser validates that the subtype header fits within the image, but does not verify that the advertised subtype length fits. A malformed CRAT table with an oversized length field causes out-of-bounds reads when kfd_parse_subtype() casts the header to specific subtype structures. Add validation that sub_type_hdr + length does not exceed the image boundary before parsing the subtype contents. (cherry picked from commit 48e1d1e6e8798aef0312e68d8e586021b5b3cf4d)	8.0	More Details
CVE-2026-86140	In libxml2 before 2.15.4, xmlSnprintfElements in valid.c has a strcat stack-based buffer overflow.	8.0	More Details
CVE-2026-52831	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.16.4, the Nuclio controller builds a curl invocation string for each cron trigger and stores it as the args of a Kubernetes CronJob container (/bin/sh, -c, <command>). Two fields in the trigger specification flow into this string without adequate sanitization: event.headers keys and event.body. This issue has been patched in version 1.16.4.	8.0	More Details
CVE-2026-52833	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.16.5, Nuclio's Java runtime generates a build.gradle file during function builds using Go's text/template package. The template renders runtimeAttributes.repositories[] values with the {{ . }} action, which performs no escaping. An attacker can embed a closing brace (}) to break out of the repositories {} block and append arbitrary Groovy statements that execute unconditionally during the Gradle configuration phase. This issue has been patched in version 1.16.5.	8.0	More Details
CVE-2026-84665	Jenkins SonarQube Scanner Plugin 2.18.3 and earlier does not limit URL schemes for the dashboard links it creates based on SonarQube scanner results, allowing the `javascript:` scheme, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	8.0	More Details
	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.17.4, on the		

CVE-2026-79755	Nuclio local Docker platform, the function namespace is interpolated—unvalidated—into a double-quoted docker ps --filter "label=nuclio.io/namespace=<value>" command that is executed via the host shell (/bin/sh -c). Because the default auth kind is nop (unauthenticated), a remote attacker can inject arbitrary OS commands that run as root inside the dashboard container, which holds the Docker socket → host compromise. This issue has been patched in version 1.17.4.	8.0	More Details
CVE-2026-78408	The nsenter --join-cgroup option opens the target cgroup.procs file as root and leaves that file descriptor open across later namespace and credential changes and across execve(). Because the kernel checks later cgroup migrations using the credentials from the original open, a program run in an attacker-controlled target can inherit root's ability to move host processes between cgroups. After a privileged operator uses --join-cgroup against that target, an unprivileged user can migrate and terminate unrelated root processes.	7.9	More Details
CVE-2026-85649	(Holloway) Chew, Kean Ho's Actualizer v1.2.0 and earlier contains a fail-open password validation vulnerability in the Alpha user and root user password loops of Shell/debian-minbase-install.sh. The installer invokes mkpasswd to generate yescrypt password hashes but does not check the command's return value and unconditionally accepts the result. If mkpasswd fails to generate a yescrypt hash, for example because an incompatible mkpasswd implementation or an environment without yescrypt support is used, the resulting password hash variable can be empty and the build proceeds. The resulting image can therefore contain empty password fields for the root and alpha accounts, potentially permitting passwordless authentication depending on the authentication configuration.	7.9	More Details
CVE-2026-6958	Acunetix 25.11.251107123 for Windows contains a local privilege escalation vulnerability in the Web Vulnerability Scanning Engine (wvsc.exe) that allows low-privileged local attackers to execute arbitrary code as SYSTEM by exploiting a missing hardcoded directory path for OpenSSL-related files. Attackers can create the missing directory, place a malicious file at the expected path, and cause the SYSTEM-level wvsc.exe process to load and execute it, resulting in full privilege escalation.	7.8	More Details
CVE-2026-78410	A flaw was found in util-linux. Restricted bind mounts take the source path from fstab but do not pin that source before the privileged mount. A local unprivileged user who can replace the authorized source or a writable ancestor can redirect SUID mount(8) to bind another host directory. If the fstab entry also sets X-mount.owner, X-mount.group, or X-mount.mode, root then changes ownership or mode on that redirected inode.	7.8	More Details
CVE-2026-80166	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Privilege Management vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	7.8	More Details
CVE-2026-64199	There is an out-of-bounds read vulnerability in DASYLab due to improper validation of user-supplied data. This results in a read outside the bounds of an allocated data structure. Successful exploitation requires an attacker to get a user to open a specially crafted .DSB file. This issue affects all versions before 2026.0.0.	7.8	More Details
CVE-2026-64200	There is an out-of-bounds read vulnerability in DASYLab due to improper validation of user-supplied data. This results in a read a past the end of an allocated heap buffer during string conversion. Successful exploitation requires an attacker to get a user to open a specially crafted .DSB file. This issue affects all versions before 2026.0.0.	7.8	More Details
CVE-2026-86504	In JetBrains IntelliJ IDEA before 2026.2.2 missing project-trust confirmation before building a Dev Container allowed host-level code execution	7.8	More Details
CVE-2026-64197	There is an out-of-bounds write vulnerability in DASYLab due to improper validation of user-supplied data, resulting in a write past the end of an allocated data structure. Successful exploitation requires an attacker to get a user to open a specially crafted .DSB file. This issue affects all versions before 2026.0.0.	7.8	More Details
CVE-2026-76967	SAP NetWeaver Business Client does not perform sufficient validation when processing certain locally stored data during application startup. An attacker with low privileges on the local system could replace this data with specially crafted content. When the application is next launched, the crafted content is processed and could lead to arbitrary code execution in the context of the user. This results in a high impact on confidentiality, integrity and availability of the application.	7.8	More Details
CVE-2026-86313	Out-of-bounds write vulnerability in Samsung Opensource Walrus allows Overflow Buffers. This issue affects Walrus: af80e665ea49d9003695a66502f841ed1d8397e7.	7.8	More Details
CVE-2026-45200	Software installed and run as a non-privileged user may conduct improper GPU driver IOCTL calls to create an allocation scenario that when freed would cause double free and kernel heap corruption. Scenario caused by fabricating a specific combination of flags on the allocation interface that would cause an incorrect double free event when freed.	7.8	More Details
CVE-2026-86540	knowns versions before 0.30.0 fail to validate the settings.lsp.languages binary field in project configuration files, allowing attackers to execute arbitrary binaries by crafting a malicious .knowns/config.json file. When a repository with a crafted configuration is opened, the unvalidated binary path is executed twice under the user's account without any verification.	7.8	More Details

CVE-2026-85439	MOOS-IvP through 24.8.1 contains a remote code execution vulnerability in alogsplit's SplitHandler::handlePreCheckSplitDir() function that fails to sanitize shell metacharacters in log file pathnames. Attackers can embed shell syntax in log file names or the --dir parameter to execute arbitrary commands with the privileges of the operator running alogsplit.	7.8	More Details
CVE-2026-64198	There is an out-of-bounds read vulnerability in DASYLab due to improper validation of user-supplied data. This results in a read a few bytes past the end of an allocated heap buffer during file handling. Successful exploitation requires an attacker to get a user to open a specially crafted .DSB file. This issue affects all versions before 2026.0.0.	7.8	More Details
CVE-2026-83959	Substance3D - Sampler is 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-2026-64196	There is an out-of-bounds write vulnerability in DASYLab due to improper validation of user-supplied data, resulting in a write past the end of an allocated heap. Successful exploitation requires an attacker to get a user to open a specially crafted .DSB file. This issue affects all versions before 2026.0.0.	7.8	More Details
CVE-2026-64195	There is an out-of-bounds write vulnerability in DASYLab due to lack of proper validation of user-supplied data. Successful exploitation requires an attacker to get a user to open a specially crafted .DSB file. This issue affects all versions before 2026.0.0.	7.8	More Details
CVE-2026-80119	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain an information disclosure vulnerability in DirectIo64.sys that allows unauthenticated local attackers to dump complete physical memory contents by supplying a caller-controlled file path to an exposed IOCTL. Attackers can issue a single IOCTL call to trigger the driver to iterate all physical memory ranges via MmGetPhysicalMemoryRanges and map each page through ZwMapViewOfSection on the PhysicalMemory section object, writing a full RAM image to an attacker-specified path in the SYSTEM context, bypassing user-mode ACLs and exposing LSASS working set, process memory, and cryptographic material from all running processes.	7.8	More Details
CVE-2026-80116	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain a privilege escalation vulnerability in DirectIo64.sys that allows local users to modify hardware configuration by exploiting exposed IOCTLs with no validation on device selection, register offset, or value. Attackers can obtain a device handle and issue arbitrary PCI configuration space read/write operations to enable Bus Master DMA on any PCI device, halt storage controller I/O by clearing command registers, or remap Base Address Registers to redirect DMA to an attacker-chosen physical address.	7.8	More Details
CVE-2026-80748	In the Linux kernel, the following vulnerability has been resolved: mmc: loongson2: Fix sg iteration in data reorder functions In ls2k0500_mmc_reorder_cmd_data() and ls2k2000_mmc_reorder_cmd_data(), the for_each_sg() macro already iterates over the scatterlist entries, with 'sg' pointing to the current entry. However, the code incorrectly uses '&sg[i]' and 'sg_dma_len(&sg[i])' inside the loop, which treats 'sg' as an array base and indexes it again, leading to access of wrong sg entries (or out-of-bounds if the list is not an array).	7.8	More Details
CVE-2026-80114	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain a hard-coded credentials vulnerability in DirectIo64.sys that allows local attackers to perform arbitrary physical memory writes by extracting an 8-byte key embedded as a hardcoded literal in the distributed binary and computing valid MD5 authentication tags for arbitrary IOCTL write requests. Attackers can additionally bypass a secondary validation gate by using the driver's own bit-clear IOCTL to clear a single bit in the gating instruction's displacement byte, causing all subsequent write requests to skip MAC verification, size checks, and Vendor ID checks entirely.	7.8	More Details
CVE-2026-80112	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain an improper access control vulnerability in the DirectIo64.sys kernel driver that allows unprivileged local users to perform privileged hardware operations by opening a handle to the device object created without a security descriptor. Attackers can issue IOCTLs through the permissive default Windows ACL applied to the device to access restricted hardware operations regardless of privilege or integrity level.	7.8	More Details
CVE-2026-85656	An OS command injection issue in the log4j-cve-2021-44228-hotpatch package in Amazon Linux before 1.3-9 might allow a local user to execute arbitrary commands with root privileges via a Java process whose executable path contains embedded newline characters.	7.8	More Details
CVE-2026-85654	Improper neutralization of special elements used in a template engine in the CDK generator in Amazon awslabs.dynamodb-mcp-server before 2.1.6 might allow a context-dependent actor to execute arbitrary code on the host that deploys the generated application via crafted table, index, or attribute names in a data model file.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: pmdomain: mediatek: mfg: initialize prev_o in mtk_mfg_attach_dev() mtk_mfg_attach_dev() reads prev_o on the first iteration of its loop, in "if (prev_o &&		

CVE-2026-80751	prev_o->freq == o->freq)", before prev_o is assigned at the end of the loop body. On that first iteration, evaluating prev_o reads an indeterminate value. If it is non-NULL, the condition dereferences a stale or invalid pointer, potentially faulting or incorrectly skipping the first OPP. Initialize prev_o to NULL. This matches the intent as well: there is no previous OPP to compare against on the first iteration. Found with Clang's -Wconditional-uninitialized.	7.8	More Details
CVE-2026-80754	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - fix F55 transmitter electrode count typo During F55 sensor detection, the transmitter (TX) electrode count was incorrectly assigned the value of the receiver (RX) electrode count due to copy-paste typos. This incorrect value was then propagated to the driver data and used by F54 to determine the diagnostics report size. On devices with more RX than TX electrodes, this inflated the perceived TX count, leading to incorrect report size calculations and potential out-of-bounds buffer accesses. Fix the typos by correctly assigning the TX electrode counts.	7.8	More Details
CVE-2026-80737	In the Linux kernel, the following vulnerability has been resolved: serial: amba-pl011: synchronize DMA teardown dmaengine_terminate_all() does not wait for a running callback, so the TX callback can still touch the TX buffer after it is freed. The RX poll timer reads the RX buffers without the port lock. Switch to dmaengine_terminate_sync() and delete the RX timer before freeing the buffers.	7.8	More Details
CVE-2026-80736	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Fix bandwidth group reservation indexing Valid bandwidth group IDs range from 1 through MAX_GROUPS, while Group ID 0 is reserved. tb_consumed_dp_bandwidth() uses the Group ID directly to index its local group_reserved[] array. The array currently has MAX_GROUPS entries, so its valid indices are 0 through MAX_GROUPS - 1. Group ID MAX_GROUPS therefore accesses one element past the end, and the final group's reserved bandwidth is not included when the array is summed. Give group_reserved[] MAX_GROUPS + 1 entries so direct Group ID indexing covers the reserved ID 0 and valid IDs 1 through MAX_GROUPS.	7.8	More Details
CVE-2026-86095	Unidata netcdf-c through 4.10.1 contains an out-of-bounds write vulnerability in NC4_HDF5_inq_attname() that copies HDF5 attribute names into a fixed 256-byte buffer without length validation. Attackers can craft HDF5 files with oversized attribute names to overflow the destination buffer, causing memory corruption and crashes when applications enumerate attribute names.	7.8	More Details
CVE-2026-80732	In the Linux kernel, the following vulnerability has been resolved: ata: pata_sl82c105: fix bridge revision use-after-free pci_get_slot() returns a referenced PCI device. Commit 44c10138fd4b ("PCI: Change all drivers to use pci_device->revision") replaced a configuration-space read with direct access to the cached revision field, but left that access after pci_dev_put(). The bridge may therefore be freed before its revision is read. Read the revision before dropping the reference.	7.8	More Details
CVE-2026-80731	In the Linux kernel, the following vulnerability has been resolved: net: remove CAP_SYS_RAWIO zero-padding in dev_validate_header dev_validate_header() reads dev->hard_header_len directly when zero-padding short link layer headers for CAP_SYS_RAWIO holders: if (capable(CAP_SYS_RAWIO)) { memset(ll_header + len, 0, dev->hard_header_len - len); return true; } Packet send paths call dev_validate_header() on skbs whose headroom was allocated from an earlier hard_header_len read. If the device is reconfigured so that dev->hard_header_len increases before validation, the memset writes past the reserved buffer, an out-of-bounds write. This out-of-bounds write is masked in some SOCK_RAW paths today because the same concurrent increase can first make skb_push() exceed the reserved headroom and trigger skb_under_panic(). Remove the zero-padding branch before making those hard_header_len reads consistent, so the snapshot fixes do not turn a loud panic into a silent overwrite. This path is only reached for variable length L2 protocols, where len < hard_header_len but len >= min_header_len. No remaining in-tree variable length L2 protocol implements header_ops->validate, and the CAP_SYS_RAWIO bypass that zero-pads and accepts short headers has no real value beyond allowing testing of intentionally malformed input. Drop the CAP_SYS_RAWIO branch. The remaining reads of dev->hard_header_len in dev_validate_header() are comparisons only and have no memory safety impact.	7.8	More Details
CVE-2026-84838	A flaw was found in rpmuncompress. This command injection vulnerability allows a local attacker to execute arbitrary commands. This occurs when rpmuncompress processes a specially crafted archive filename containing shell metacharacters, which are not properly escaped before being passed to shell command strings. Successful exploitation requires user interaction, where a user or automated workflow invokes rpmuncompress on the malicious file, leading to high impact on the confidentiality, integrity, and availability of data accessible to the invoking user.	7.8	More Details
CVE-2026-78604	Incorrect Permission Assignment for Critical Resource (CWE-732) in Elastic Agent can lead to local privilege escalation via Replace Binaries (CAPEC-642). On Windows systems where Elastic Agent is installed in unprivileged mode, resources used by the agent service are created with access controls broader than required. A local user could take advantage of this to cause the service to execute code of their choosing, ultimately obtaining SYSTEM-level privileges on the host.	7.8	More Details
CVE-2026-85028	Creation of a temporary file in a directory with insecure permissions in the FPGA management tool installation component in AWS FPGA Development Kit (aws-fpga) before 2.3.4 might allow local users to execute arbitrary code with root privileges via crafted shell content placed at a predictable path in a world-writable temporary directory, which the installation step reads after elevating its own privileges. To remediate this issue, users should upgrade to version 2.3.4.	7.8	More Details

CVE-2026-85690	Plandex 2.2.1 contains a path traversal vulnerability in the ApplyFiles function that allows attackers to write files outside the project directory. Attackers can influence model output through poisoned repository files or attacker-controlled context to write to arbitrary locations like shell rc or cron files, achieving code execution.	7.8	More Details
CVE-2026-76642	util-linux versions through 2.41.5 and 2.42.2 fail to check mount helper exit status before running post-mount hooks, allowing unprivileged users to execute privileged operations on pre-existing filesystems. Attackers can exploit X-mount.idmap or X-mount.owner hooks to clone filesystems with inherited suid bits or modify target inode permissions after a helper fails, achieving privilege escalation.	7.8	More Details
CVE-2026-84837	A flaw was found in rpm. An attacker can exploit a command injection vulnerability by influencing the path or filename of a tarball processed by `rpmbuild -t*` to include shell metacharacters. This is particularly relevant in automated build or continuous integration (CI) workflows that ingest externally supplied artifact names. Successful exploitation allows for arbitrary command execution with the privileges of the build user, which could lead to information disclosure or disruption of the build environment.	7.8	More Details
CVE-2026-73600	Dell PowerProtect Data Manager, versions 20.2.0.0 and below, contain a stack buffer overflow vulnerability in file-level restore agent. A high privileged remote attacker could potentially exploit this vulnerability, leading to Information disclosure.	7.8	More Details
CVE-2026-85674	aider (aider-chat) automatically loads a .aider.conf.yml configuration file from the root of the git repository it is launched in. A crafted repository can set test-cmd (executed at startup) or lint-cmd (executed on the first file edit), which aider runs through a shell (subprocess with shell=True) without any user confirmation, LLM interaction, or API key. Consequently, a user who clones and runs aider inside an attacker-supplied repository achieves arbitrary command execution on their machine. The behavior is long-standing and was confirmed on 0.86.3.dev (current main).	7.8	More Details
CVE-2026-86494	In JetBrains YouTrack before 2026.2.18634 cloning a whiteboard allowed unauthorized changes to links on inaccessible issues	7.7	More Details
CVE-2023-20576	Insufficient Verification of Data Authenticity in AGESA™ may allow an attacker to update SPI ROM data potentially resulting in denial of service or privilege escalation.	7.7	More Details
CVE-2026-75033	A flaw was found in Rancher Manager. Project Secrets were propagated into a namespace based only on its `field.cattle.io/projectId` annotation, without verifying that the referenced project belonged to the same downstream cluster. A user able to create namespaces on one cluster could set the annotation to a project ID from another cluster and have that project's secrets copied into a namespace under their control. This issue affects Rancher: before 2.15.1.	7.7	More Details
CVE-2026-66767	SAP NetWeaver Application Server for ABAP and ABAP Platform allows an unauthenticated user to send a specially crafted packet that triggers reprocessing of a previously buffered user request, potentially hijacking another user's session under narrow timing conditions. Successful exploitation could result in high impact on confidentiality and integrity, with low impact on availability of the application.	7.7	More Details
CVE-2026-85178	Helicone's VaultManager.getDecryptedProviderKeyById() function in the GET /v1/vault/key/{providerKeyId} endpoint fails to validate the requester's organization against the vault key's organization identifier. Attackers with admin or owner privileges in any organization can retrieve decrypted upstream provider credentials for other tenants, including plaintext OpenAI, Anthropic, and Bedrock API keys.	7.7	More Details
CVE-2026-55658	Gardens v2 is a modular governance framework that enables communities to create and manage multiple governance pools with customizable parameters and voting mechanisms. In 3e595f3 and prior, when a streaming proposal is funded, the cluster of streaming contracts moves real pool funds into the proposal's StreamingEscrow to back the Superfluid constant flow agreement (the CFA deposit, plus a 0.5 percent margin). cancelProposal then zeroes the escrow's GDA member units but never reclaims that parked balance, and the permissionless claim() forwards the escrow's entire balance, including the pool funded buffer, to the beneficiary. The beneficiary is chosen by the proposal submitter and defaults to the submitter. The only path that returns escrow funds to the pool is drainToStrategy, which is onlyStrategy and is reached solely from the dispute reject ruling, never from cancel or natural completion. At time of publication, there are no publicly known patches.	7.7	More Details
CVE-2026-86498	In JetBrains YouTrack before 2025.3.160480, 2026.1.14047 pUT requests on link sub-resources allowed modification linked entities without update permission	7.7	More Details
CVE-2026-85211	Label Studio fails to apply organization filters when resolving storage URIs for tasks and projects in proxy_api.py endpoints. Attackers can access other tenants' cloud storage objects by creating a separate organization and supplying arbitrary file URIs to presign or stream bucket contents.	7.7	More Details
CVE-2026-75035	A flaw was found in Rancher Manager. When a non-administrative caller supplied a label selector naming a different user, the ext.cattle.io/v1 Token store dropped its internal owner filter instead of returning an empty result. Any authenticated user could therefore list and watch every other user's tokens, disclosing token	7.7	More Details

	metadata and the stored salted hash of the bearer token. This issue affects Rancher: before 2.15.1.		
CVE-2026-19306	IBM Langflow OSS 1.0.0 through 1.11.2 allows an authenticated attacker to read arbitrary files from the server filesystem — including server secret material (secret_key, JWT signing keys, the application database, /proc/self/environ, and other tenants' upload directories) — by supplying absolute paths or traversal sequences in the files parameter of an authenticated build request. The file contents were embedded as text attachments in the language model prompt and transmitted to the configured model endpoint, resulting in confidential data exfiltration. This bypassed the LANGFLOW_RESTRICT_LOCAL_FILE_ACCESS=true containment boundary, which was enforced for other file-reading components but not for the Chat Input to Message attachment pipeline.	7.7	More Details
CVE-2026-80134	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Use of Hard-coded Credentials vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.7	More Details
CVE-2026-18905	IBM ContextForge MCP Gateway (`mcp-contextforge-gateway`) <= v1.0.6 MCP Context Forge could allow a remote authenticated attacker to obtain sensitive information due to a DNS rebinding vulnerability during tool invocation.	7.7	More Details
CVE-2026-63464	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. From version 0.6.0 to before version 0.7.2, non-admin operators (role user) can set allow_private: true on their own managed webhook subscription (POST/PATCH /api/v1/webhook-subscriptions). No admin check exists on this field. At delivery time, allow_private switches the dispatcher to an unguarded HTTP client, bypassing the private/loopback/link-local SSRF guard — letting a low-privilege operator make the server request internal addresses. This issue has been patched in version 0.7.2.	7.7	More Details
CVE-2026-19304	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote authenticated attacker to obtain sensitive information from internal services due to a URL parser discrepancy.	7.7	More Details
CVE-2026-81832	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 SAP Adapter is vulnerable to an XML external entity (XXE) attack.	7.7	More Details
CVE-2026-19283	IBM Observability with Instana (Agent) Build 1.0.303 through 1.0.323 IBM Instana Agent Operator could allow an authenticated remote attacker to obtain sensitive information, caused by missing destination namespace validation when copying etcd mTLS client credentials from the openshift-etcd system namespace into an attacker-controlled namespace.	7.7	More Details
CVE-2026-85213	Kill Bill through 0.24.21 fails to enforce permission annotations on several AdminResource endpoints including getQueueEntries, invalidatesCache, and putOutOfRotation. Authenticated users with minimal account:read permissions can read internal queues, flush server caches, and disable the server by putting the host out of rotation.	7.6	More Details
CVE-2026-53635	Open edX Platform enables the authoring and delivery of online learning at any scale. Prior to commit 59bb6d6, the view function set_course_mode_price() at lms/djangoapps/instructor/views/instructor_dashboard.py:430 is decorated only with @login_required and performs no course-level permission check. Any authenticated user — including a learner account with zero course roles — can issue a single POST request to overwrite the honor mode price and currency of any course on the platform. The companion frontend modal was removed in a prior cleanup, but the URL route and view remain live, making this an unguarded orphan endpoint. This issue has been patched via commit 59bb6d6.	7.6	More Details
CVE-2026-57777	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Automattic WooCommerce allows Blind SQL Injection. This issue affects WooCommerce: from n/a before 11.0.	7.6	More Details
CVE-2026-85197	A flaw was found in libsoup. A malicious HTTP/2 server or a Man-in-the-Middle (MITM) attacker can exploit a heap use-after-free vulnerability in the HTTP/2 client implementation. This occurs when a GNOME application uploads a file using HTTP/2, and the server sends a GOAWAY frame while the file body is being read asynchronously. This can lead to memory corruption, potentially resulting in information disclosure or arbitrary code execution.	7.6	More Details
CVE-2025-46418	Westermo WeOS 5.x starting from 5.24 allows OS command injection via a media definition.	7.6	More Details
CVE-2026-79639	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.6	More Details
CVE-2026-	Unauthenticated Denial of Service Attack in Migrate Guru – Site Migration & Cloning <= 6.65 versions.	7.5	More Details

84778			
CVE-2026-16025	Improper validation of specified quantity in input vulnerability in PayTR Payment and Electronic Money Institution Inc. PayTR Virtual Pos iFrame API (v9x) WHMCS Module allows Input Data Manipulation. This issue affects PayTR Virtual Pos iFrame API (v9x) WHMCS Module: from v9.0.0 before v9.0.3.	7.5	More Details
CVE-2026-85671	QAnything 2.0.0 contains an authentication bypass vulnerability in the /api/local_doc_qa/get_file_base64 and /api/local_doc_qa/get_doc endpoints that allows unauthenticated attackers to access any uploaded file or document. Attackers can enumerate file identifiers through unauthenticated endpoints and retrieve base64-encoded files or parsed document chunks without ownership verification to disclose cross-tenant knowledge base content.	7.5	More Details
CVE-2026-84776	Unauthenticated Denial of Service Attack in MalCare Security <= 6.69 versions.	7.5	More Details
CVE-2026-85673	LLaMA-Factory contains a server-side request forgery vulnerability in the OpenAI-compatible API multimodal media URL handler that allows unauthenticated attackers to bypass SSRF validation. The check_ssrf_url guard validates URLs once but requests.get follows redirects and re-resolves DNS without re-validation, enabling attackers to use HTTP redirects or DNS rebinding to access internal addresses and cloud metadata endpoints.	7.5	More Details
CVE-2026-85675	OWL's DocumentProcessingToolkit contains a server-side request forgery vulnerability in the extract_document_content tool that fetches caller-supplied URLs with no scheme, host, or IP filtering. Attackers can inject malicious URLs through prompt injection to make the server fetch internal resources, with responses returned to the agent context.	7.5	More Details
CVE-2026-16037	Observable timing discrepancy vulnerability in PayTR Payment and Electronic Money Institution Inc. PayTR Virtual Pos iFrame API (v9x) WHMCS Module allows Black Box Reverse Engineering. This issue affects PayTR Virtual Pos iFrame API (v9x) WHMCS Module: from v9.0.0 before v9.0.3.	7.5	More Details
CVE-2026-85685	AgentScope through 2.0.7.post1 contains a path traversal vulnerability in LocalWorkspace.add_skill that copies arbitrary server directories into the agent workspace via an unconfined source path parameter. Attackers can supply any directory path in the skill_path request parameter to copy files into the skills directory, making them accessible through the workspace skill listing.	7.5	More Details
CVE-2026-48486	Signum Node is a HDD-mined cryptocurrency using an energy efficient and fair Proof-of-Commitment (PoC+) consensus algorithm. Prior to version 3.9.9, an integer overflow in BlockServiceImpl.applyBlock() allowed a miner to receive an arbitrarily inflated block reward by crafting a block with a negative totalFeeCashBackNqt value. The vulnerability was introduced when the SMART_FEES hardfork (block ~1,029,000) enabled fee cash-back and burn accounting without overflow protection. This issue has been patched in version 3.9.9.	7.5	More Details
CVE-2026-85609	Openpanel before 2.3.0 contains an unauthenticated full-read server-side request forgery (SSRF) vulnerability in the GET /tools/site-checker endpoint (apps/api/src/controllers/tools.controller.ts). The endpoint passes a user-supplied url query parameter to fetchWithRedirects() and performs server-side HTTP requests to arbitrary URLs without any SSRF/IP validation. An unauthenticated remote attacker can access cloud instance metadata endpoints, probe internal services, scan internal network ports, and read returned content (status code, page size, timing, and parsed HTML metadata), and leak internal IP addresses (via getIPInfo() to a third party).	7.5	More Details
CVE-2026-85668	Xinference (affected commit 4a94832, v3.x) contains an unauthenticated arbitrary-path file read vulnerability in the POST /v1/models/llm/auto-register endpoint, which accepts a caller-supplied model_path parameter without authentication or path confinement. The endpoint reads and parses config.json, tokenizer_config.json, and chat_template.jinja files at the supplied path and reflects the parsed content back to the caller, allowing an unauthenticated attacker to probe the server filesystem and extract content of files with those names in any directory.	7.5	More Details
CVE-2026-79377	A heap overflow in the a2dp_decoder_sbc.cpp component of Bestechnic Co., Ltd BES2300 Bluetooth Audio SoC firmware v3.x and earlier allows attackers to cause a Denial of Service (DoS) via sending a crafted L2CAP packet.	7.5	More Details
CVE-2026-84847	Unauthenticated Broken Access Control in Quick Event Manager <= 9.17 versions.	7.5	More Details
CVE-2026-85666	OGX (formerly Llama Stack, affected at commit fbe8e0f) contains an unauthenticated server-side request forgery vulnerability in the OpenAI-compatible POST /v1/responses endpoint. MCP tool definitions accept a server_url parameter (along with headers and authorization values) that is fetched server-side without destination validation; the existing validate_url_not_private() guard used for other URL inputs is not applied to server_url. On the default starter configuration, which runs without authentication, a remote unauthenticated attacker can cause the server to open connections to arbitrary internal addresses (including cloud metadata endpoints such as http://169.254.169.254/) and forward attacker-supplied headers and bearer tokens to those destinations.	7.5	More Details

CVE-2026-85664	Chroma 1.5.9 fails to validate maximum bounds on HNSW index parameters max_neighbors, ef_construction, and ef_search in collection-create requests. Unauthenticated attackers can supply arbitrarily large parameter values to exhaust server memory and cause denial of service during index compaction.	7.5	More Details
CVE-2026-33630	c-ares is an asynchronous resolver library. From ver 1.32.3 until 1.34.7, a use-after-free / double-free in c-ares' query-completion handling. The same flaw — a query's callback being invoked while the query is still linked in the channel's internal lookup structures — is present at multiple points in the resend/finish path (timeout handling, response handling, and query dispatch). If the query, or for ares_getaddrinfo() the owning host_query, is freed as a side effect of that callback, it is then accessed and/or freed a second time. This vulnerability is fixed in ver 1.34.7.	7.5	More Details
CVE-2026-73316	XenForo before 2.3.13 contains a payment replay vulnerability in the PayPal REST payment provider that allows attackers to process the same webhook payload multiple times by exploiting a missing duplicate transaction ID check. Attackers can replay a valid webhook payload to trigger duplicate payment events, resulting in repeated subscription activations and unauthorized account upgrades.	7.5	More Details
CVE-2026-73314	XenForo before 2.3.13 contains a signature verification logic error in the PayPal REST webhook handler that allows unauthenticated attackers to bypass payment signature validation by submitting a webhook request with an unsupported auth_algo header value. When the algorithm cannot be mapped to a supported hash function, the verification function incorrectly returns true instead of failing, causing the caller to treat the fabricated request as verified and process the payment event without a valid PayPal signature.	7.5	More Details
CVE-2026-18056	The HivePress Authentication plugin for WordPress is vulnerable to Authentication Bypass via the access_token parameter in all versions up to, and including, 1.1.4. This is due to the authenticate_user function's Facebook authenticator resolving third-party identity by forwarding the attacker-supplied access_token to the Facebook Graph API and trusting the returned email and ID verbatim, without performing any application ID or audience validation — specifically, no /debug_token verification and no comparison of the token's app_id against the configured hp_facebook_app_id. This makes it possible for unauthenticated attackers to authenticate as any existing WordPress user, including administrators, whose email address is associated with a Facebook account for which the attacker can obtain any valid access token. Important Note: To exploit the vulnerability, the attacker must obtain the victim's access token.	7.5	More Details
CVE-2026-33389	An improper certificate/host key validation vulnerability was discovered in the Smart Polling functionality, which established encrypted connections to target devices without validating the remote host's identity, and no option was provided to enable it. A man-in-the-middle attacker positioned between a sensor and a polled device can, during a polling session, impersonate the device and intercept the communication, including the credentials used to access it. The captured credentials can then be replayed to authenticate against the device itself or against other devices sharing the same credentials, allowing the attacker to access and tamper with the device's data and to disrupt its operations.	7.5	More Details
CVE-2026-85393	node-forge through 1.4.0 fails to validate element count in nested DigestAlgorithm sequences during RSA PKCS#1 v1.5 signature verification. Attackers can embed garbage bytes inside the DigestAlgorithm sequence to forge valid signatures for arbitrary messages using low-exponent RSA keys. This is an incomplete fix for CVE-2026-33894.	7.5	More Details
CVE-2026-85396	rubyzip versions before 3.4.0 contain a path traversal vulnerability in Zip::Entry#extract that fails to properly validate extraction paths using prefix comparison without trailing separators. Attackers can craft archive entries with names like ../upload_backup/owned.sh to write files outside the intended extraction directory into sibling paths sharing the destination prefix.	7.5	More Details
CVE-2026-84219	The Kirki WordPress plugin before 6.3.0 does not hold back every spelling of the HTML entities it decodes when rendering, allowing unauthenticated users to store JavaScript in a comment which then runs in the session of anyone viewing a page that displays it, including an administrator, and on every page of the site when its header or footer is built to show comments.	7.5	More Details
CVE-2026-82527	R2R through 3.6.6 contains a SQL injection vulnerability that allows unauthenticated attackers to inject SQL predicates into the chunks search query by manipulating the filter key parameter in the retrieval search endpoint. Attackers can exploit the direct interpolation of filter keys into the SQL WHERE clause without parameterization or escaping to perform time-based and boolean-based data exfiltration from the application database.	7.5	More Details
CVE-2026-85045	Race condition in V8 in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-85626	git-mcp-server 2.15.1 contains an argument injection vulnerability in the ref and object parameters of git_log, git_diff, and git_show tools that lack leading-dash validation. Attackers can inject git command-line options like --output= to write files outside the repository to arbitrary paths accessible by the process.	7.5	More Details
CVE-2026-	ms-swift 4.5.2 contains a server-side request forgery vulnerability in the swift deploy OpenAI-compatible API that fetches multimodal media URLs without validation or redirect filtering. Unauthenticated attackers can supply arbitrary image_url, audio_url, or video_url parameters to make the server issue requests to internal	7.5	More Details

85686	services and cloud metadata endpoints.		
CVE-2026-85180	Ollama fails to validate redirect destinations when pulling tensor-layer models, allowing unauthenticated attackers to redirect blob downloads to arbitrary hosts. An attacker can control a registry, serve a malicious tensor-layer manifest, and cause the server to issue GET requests to internal hosts including cloud metadata endpoints.	7.5	More Details
CVE-2026-86721	AVideo through commit c3edcc274c contains an authorization bypass vulnerability where a session cookie named 'key' with value 'value' overrides the $_REQUEST['key'] parameter in saveLive.php and related endpoints. Attackers can publish to any user's RTMP stream without authentication by using the known constant stream key value to hijack live broadcasts.	7.5	More Details
CVE-2026-85687	surya 0.22.1 screenshot server contains an unauthenticated arbitrary file read vulnerability in the /info, /page, and /process routes that accept raw file_path parameters. Attackers can read any image or PDF file on the host by supplying arbitrary file paths to Image.open or pypdfium2.PdfDocument, obtaining rendered contents as base64 and using /info as an existence oracle.	7.5	More Details
CVE-2026-71626	An issue in Invoice Ninja v5.13.24 allows a remote attacker to obtain sensitive information via the StoreWebhookRequest.php, UpdateWebhookRequest.php, and WebhookSingle.php components	7.5	More Details
CVE-2026-85786	Improper handling of highly compressed data in Amazon ion-java before 1.12.1 might allow remote attackers to cause a denial of service via a crafted compressed Ion document that expands to an arbitrarily large size upon decompression due to insufficient coverage of the GZIP auto-decompression opt-out introduced for CVE-2026-75936. To remediate this issue, users should upgrade to version 1.12.1.	7.5	More Details
CVE-2026-82075	An uncontrolled resource consumption weakness exists in the request-handling path of the MongoDB sharded-cluster router process. A client that has network access to a router port and has not authenticated can supply connection-monitoring parameters that cause the server to expend CPU resources without any rate limiting, degrading or denying service to legitimate clients. No authentication, elevated privileges, or user interaction is required. Only availability is affected; data confidentiality and integrity are not impacted.	7.5	More Details
CVE-2026-61686	SolidInvoice is an open-source invoicing platform. Prior to version 3.0.1, the `DataGrid` LiveComponent deserializes a `context` prop value using PHP's `unserialize()` after receiving it from the client. Because the prop is marked `writable: true`, an authenticated attacker can supply an arbitrary PHP serialized payload. Version 3.0.1 fixes the issue.	7.5	More Details
CVE-2026-19534	undici's WebSocket client crashes the whole Node.js process during the opening handshake when a server responds with a subprotocol that the client never requested. A default WebSocket connection sends no subprotocol, but if the server's 101 response includes a Sec-WebSocket-Protocol header, undici dereferences a null value while checking it against the requested list and throws an uncaught TypeError. Because that code runs inside a microtask with no surrounding error handling, the exception propagates and terminates the process under Node's default behavior, instead of gracefully failing the connection as required by the WebSocket protocol. Any application that opens a WebSocket to an attacker-controlled or compromised server, or over a plaintext connection subject to a machine-in-the-middle, can be crashed remotely without authentication in the default configuration. This affects undici versions from 6.7.0 up to 6.28.1, from 7.0.0 up to 7.29.1, and from 8.0.0 up to 8.10.2. Users should upgrade to undici 6.28.1, 7.29.1, or 8.10.2.	7.5	More Details
CVE-2026-85124	@fastify/http-proxy versions before 11.6.2 do not validate proxied HTTP request paths for backslash based dot-segments before forwarding them to the configured upstream. The plain HTTP request handler skips the destination validation that the WebSocket path performs, and the underlying reply-from library only rejects forward-slash traversal, so a request containing backslash dot-segments can escape the boundary set by the prefix and rewritePrefix options. An unauthenticated network attacker can use this to reach upstream paths that were meant to stay hidden behind the proxy, resulting in disclosure of internal endpoints. This is a path traversal issue (CWE-22). Users should upgrade to @fastify/http-proxy 11.6.2 or later.	7.5	More Details
CVE-2021-44320	Parrot AR.Drone version 1 and 2 does not employ a suitable mechanism to prevent denial-of-service (DoS) attacks. An attacker can harm the device availability (i.e., video streaming and control) by using tool to perform an IPv4 flood attack. Verified attacks includes SYN flooding and UDP flooding.	7.5	More Details
CVE-2021-44319	Parrot AR.Drone 1 and AR.Drone 2 are vulnerable to Denial of Service. The Parrot AR.Drone platform is vulnerable to Wi-Fi deauthentication attack, allowing remote and unauthenticated attackers to disconnect drone from controller during mid-flight.	7.5	More Details
CVE-2026-85150	A NULL pointer dereference flaw was found in GStreamer's RTSP support library. The vulnerability occurs while parsing an Authorization or WWW-Authenticate header that uses Digest authentication. Specially crafted whitespace placement around a parameter's terminator can cause an internal length calculation to underflow, leading to a crash of the process parsing the header. On an RTSP server this can be triggered by a remote, unauthenticated attacker sending a single malformed request when the server has authentication enabled; the same flaw can also be triggered against an RTSP client by a malicious or compromised RTSP server. Successful exploitation results in a denial of service (application crash) and has no confirmed impact on confidentiality or integrity.	7.5	More Details

CVE-2026-75438	Buffer Overflow vulnerability in Open5GS v2.7.7 allows a remote attacker to cause a denial of service via the ogs_sbi_time_parse() function	7.5	More Details
CVE-2026-85155	WWBN AVideo contains a SQL injection vulnerability in the sort column parameter of the get.json.php endpoint with APIName=channels that allows unauthenticated attackers to order results by arbitrary database columns including users.password and users.recoverPass. Attackers can exploit this ordering oracle to infer password hash values and recovery tokens, and trigger SQL errors that disclose the full query statement and database schema.	7.5	More Details
CVE-2026-13297	IBM Verify Identity Access Advanced Access Control may be vulnerable to an information disclosure attack.	7.5	More Details
CVE-2026-52770	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, YesWiki's public Bazar entry-listing APIs are vulnerable to unauthenticated SQL injection in numeric query / queries filters. For Bazar fields whose value structure is numeric, YesWiki escapes the attacker-controlled filter value but inserts it into SQL without quotes or numeric validation. An unauthenticated attacker can inject boolean SQL expressions and infer database contents from whether entries are returned. This issue has been patched in version 4.6.6.	7.5	More Details
CVE-2026-82064	A security issue in MongoDB Server allows an unauthenticated network user to cause a denial of service on a specific type of replica set member. The server contains an assertion in its read concern processing logic that can be reached without authentication, and the assertion's assumptions about internal state do not hold for all member configurations, causing the server process to terminate.	7.5	More Details
CVE-2026-19858	The JetFormBuilder — Dynamic Blocks Form Builder WordPress plugin before 3.6.5.2 does not perform authorisation checks when resolving request-derived data during page rendering, allowing unauthenticated users to read arbitrary user, post and term properties and metadata, including password hashes, private and draft content, and secrets other JetFormBuilder — Dynamic Blocks Form Builder WordPress plugin before 3.6.5.2 store in metadata.	7.5	More Details
CVE-2026-19300	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote attacker to obtain sensitive information due to incomplete scrubbing of sensitive credential fields.	7.5	More Details
CVE-2026-47625	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could abuse missing authorization. A successful exploit of this vulnerability might lead to information disclosure, data tampering, and denial of service.	7.5	More Details
CVE-2026-16497	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could cause excessive iteration. A successful exploit of this vulnerability might lead to denial of service.	7.5	More Details
CVE-2026-86728	AVideo through 29.0 contains an authentication bypass vulnerability in plugin/PlayLists/epg.json.php that exposes live-stream keys and private EPG schedules to unauthenticated users. Attackers can request the endpoint with sequential user or playlist IDs to retrieve sensitive credentials, server identifiers, and complete programme schedules without authentication.	7.5	More Details
CVE-2026-86727	AVideo through 29.0 contains an information disclosure vulnerability in plugin/Live/stats.json.php that allows unauthenticated attackers to retrieve stream keys and m3u8 URLs by accessing the endpoint without authentication. Attackers can enumerate private, unlisted, and group-restricted live streams by parsing the hidden_applications array in the JSON response to obtain sensitive streaming credentials.	7.5	More Details
CVE-2026-85699	jina-ai reader contains a server-side request forgery vulnerability where URL validation is performed only on the initial request but not re-applied to subsequent redirect hops. Attackers can craft a public URL that redirects to internal network addresses or cloud metadata endpoints, allowing the server to fetch and return the target's response body to the attacker.	7.5	More Details
CVE-2026-86173	MindsDB through 26.1.0 contains a server-side request forgery vulnerability in the web crawler handler that allows unauthenticated attackers to fetch arbitrary URLs by supplying caller-controlled URLs to CrawlerTable.list. Attackers can bypass the allowlist control by exploiting the default empty configuration and access internal services and cloud metadata endpoints without authentication.	7.5	More Details
CVE-2026-62649	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). The web server does not properly limit or manage system resources when processing a high volume of concurrent HTTP requests. This could allow an unauthenticated remote attacker to cause the entire device to crash and reboot, resulting in a denial-of-service condition.	7.5	More Details
CVE-2026-85182	vhr through commit 03abbd3 fails to verify that the account ID in PUT /hr/pass requests belongs to the authenticated caller. Authenticated attackers can change arbitrary account passwords by supplying a target account ID and that account's current password in the request body.	7.5	More Details
CVE-	MegaParse 0.0.55 contains an unauthenticated server-side request forgery vulnerability in the POST /v1/url		More

2026-85691	endpoint that fetches caller-supplied URLs server-side. Attackers can supply internal service URLs or metadata endpoints without authentication to read their responses directly from the JSON response.	7.5	Details
CVE-2026-3174	The Event Tickets and Registration plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the Stripe OAuth return endpoint in all versions up to, and including, 5.27.4. This makes it possible for unauthenticated attackers to overwrite the site's Stripe merchant credentials (access tokens, publishable keys, and account ID), diverting all subsequent payment processing to the attacker's Stripe account.	7.5	More Details
CVE-2026-48888	Allocation of Resources Without Limits or Throttling vulnerability in Automattic WooCommerce allows HTTP DoS. This issue affects WooCommerce: from n/a before 11.1.0.	7.5	More Details
CVE-2026-62648	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). The length of the URL component contained in pre-authenticated HTTP messages is not properly validated before appending additional data to it, resulting in an out-of-bounds write condition in memory. This could allow an unauthenticated remote attacker to crash the affected device, causing a reboot and resulting in a denial-of-service condition.	7.5	More Details
CVE-2026-85449	MOOS-IvP pMarineViewer through 24.8.1 fails to limit the number of tracked node identities from NODE_REPORT messages, allowing attackers to exhaust memory by supplying unbounded distinct node names. Attackers can publish crafted NODE_REPORT data to cause memory exhaustion and stall the operator display without authentication.	7.5	More Details
CVE-2026-86287	Net::IP::LPM versions before 1.12 for Perl accept malformed prefix lengths. Non-numeric and non-ASCII prefix lengths are accepted and treated as 0. Integers over 31 bits are silently truncated. A single malformed mask will poison the lookup table. The result is that the lookup will silently succeed for every address. An allow-list will allow every address, and a deny-list will block every address.	7.5	More Details
CVE-2026-16028	Protocol::HTTP2 versions before 1.14 for Perl allow memory exhaustion via closed streams that stream_state never removes from the connection stream table. When a stream reaches the CLOSED state, stream_state returns the concurrency slot and clears most of the stream's keys, but the entry itself stays in the connection stream table and nothing in the distribution removes it. Stream identifiers increase monotonically, so a peer can open and close streams on one connection indefinitely, each close leaving a residual entry that is retained for the life of the connection. SETTINGS_MAX_CONCURRENT_STREAMS does not bound this. That setting caps how many streams are live at once and is enforced, while the growth is made of streams the cap has already released, so it accumulates with concurrency never exceeding one. The client keeps the same table and grows the same way against a hostile server. Measured against a server built on this module, roughly 920 bytes are retained per closed stream for about 19 bytes on the wire, so 100,000 sequential streams on one connection grow server resident memory by about 88 MiB. The streams are ordinary requests that the application accepts and completes.	7.5	More Details
CVE-2026-19205	Observable response discrepancy vulnerability in GastroMenum GastroMenum Web Panel allows Account Footprinting. This issue affects GastroMenum Web Panel: before 31.08.2026.	7.5	More Details
CVE-2026-85147	SmartIT Desktop Manager developed by Lightstar has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can obtain a specific password from the source code, which can be used to retrieve the AES encryption key used for communication.	7.5	More Details
CVE-2026-85505	ipmi-oem in FreeIPMI before 1.6.19 has a stack-based buffer over-read in ipmi_oem_fujitsu_get_sel_entry_long_text in ipmi-oem/ipmi-oem-fujitsu.c when a BMC provides a short response, a different vulnerability than CVE-2026-50031 (which has different affected versions).	7.5	More Details
CVE-2026-81270	Apache Allura: exposure of non-public information via search. This issue affects Apache Allura: through 1.20.0. Users are recommended to upgrade to version 1.21.0, which fixes the issue.	7.5	More Details
CVE-2026-12483	The LearnDash LMS plugin for WordPress is vulnerable to Unrestricted File Type Upload in versions up to and including 5.1.5. This is due to insufficient input validation in the 'learndash_fileupload_process' function, which iterates through an entire array and validates only the first file. This makes it possible for authenticated attackers, with subscriber-level access and above who are enrolled in a course with assignment uploads enabled, to upload arbitrary disallowed files, including PHP files, to the server's wp-content/uploads/learndash/assignments/ directory. The uploaded files can only be used for Remote Code Execution if default server configurations have been changed to allow for execution.	7.5	More Details
CVE-2026-81665	A heap-based buffer overflow was found in Corosync's Totem Process Group (totempg) message reassembly. When processing fragmented multicast messages, the buffer used to reassemble fragments lacks a runtime bounds check in release builds. A network-adjacent attacker able to send crafted multicast protocol messages to the cluster could cause a heap buffer overflow with attacker-controlled data. This can crash the Corosync daemon, causing a denial of service to the entire cluster, and may potentially allow further exploitation given sufficient heap-corruption control.	7.5	More Details
CVE-	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00,		

2026-80135	contains an Improper Check or Handling of Exceptional Conditions vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	7.5	More Details
CVE-2026-86428	commonmark versions from 1.5.0 before 2.10.0 contain a denial of service vulnerability in the AttributesExtension when processing distinctly-named attributes. Attackers can submit Markdown with numerous distinct attribute names to cause quadratic-time attribute merging and filtering, consuming disproportionate CPU resources and preventing legitimate requests from completing.	7.5	More Details
CVE-2026-84469	fastify versions before 5.12.2 decide whether to compile a request schema based on JavaScript truthiness, but JSON Schema Draft 7 defines the boolean false as a valid schema that rejects every instance. When an application assigns false to a route's body, querystring, params, or headers schema to deny all input, fastify treats it as a missing schema, compiles no validator, and runs the route handler on any request. An unauthenticated remote client can therefore reach a handler that a valid deny-all schema was intended to make unreachable, a complete validation bypass that can lead to unauthorized state changes or execution of disabled operations. Users should upgrade to fastify 5.12.2 or later.	7.5	More Details
CVE-2026-85612	OpenPanel before 2.3.0 contains an unauthenticated server-side request forgery vulnerability in the /misc/favicon and /misc/og endpoints that accept an attacker-supplied url parameter with insufficient validation. Attackers can force the API to fetch arbitrary internal hosts and cloud metadata endpoints, with small responses returned verbatim enabling credential theft and internal service enumeration.	7.5	More Details
CVE-2026-86429	The league/commonmark (thephpleague/commonmark) library in versions >= 1.5.0 and < 2.9.1 contains quadratic parsing complexity in its SmartPunctExtension and AttributesExtension. When either extension is explicitly registered on the Environment (they are not enabled by default and are excluded from the standard CommonMark and GitHub-Flavored Markdown converters), an unauthenticated attacker can submit small, specially crafted Markdown documents — such as text alternating with unpaired quotes, contiguous runs of block-level attribute blocks, or repeated class attributes — to trigger disproportionate CPU consumption and cause a denial of service. Fixed in 2.9.1.	7.5	More Details
CVE-2026-86430	league/commonmark versions before 2.9.1 contain multiple denial of service vulnerabilities in fenced code block detection, reference link label lookup, and emphasis delimiter processing that perform super-linear work on crafted input. Attackers can submit specially crafted Markdown with long backtick runs, nested brackets, or delimiter sequences to consume disproportionate CPU time and prevent legitimate requests from completing.	7.5	More Details
CVE-2026-86433	commonmark versions from 1.5.0 before 2.8.4 contain a denial of service vulnerability in the Attributes extension where AttributesListener::findTargetAndDirection() performs quadratic-time sibling list scanning. Unauthenticated attackers can submit approximately 32 KB of repeated attribute blocks to cause parsing to take over 5 seconds, exhausting server resources.	7.5	More Details
CVE-2026-86434	league/commonmark versions >= 2.0.0 and < 2.8.4 (patched in 2.9.0) contain a denial of service vulnerability in UniqueSlugNormalizer::normalize(), which restarts its numeric-suffix search from 1 on every slug collision, resulting in O(K^2) time complexity for K headings that collapse to the same base slug. The vulnerable path is reached when HeadingPermalinkExtension, FootnoteExtension, or TableOfContentsExtension is registered. An unauthenticated attacker can force many headings onto a single base slug (e.g., via empty ATX headings, identical heading text, or punctuation-only headings) in a small Markdown document, consuming excessive CPU and denying service.	7.5	More Details
CVE-2026-84428	fastify versions before 5.12.2 implement the case-insensitive nature of HTTP header names by lowercasing names in a route's header schema before compiling it, but the transformation is incomplete: it lowercases the properties keys and the root-level required array, and does not lowercase the trigger and dependent names inside the JSON Schema Draft 7 dependencies keyword. Because Node stores request header names in lowercase, a canonical-case dependency such as requiring an authentication header whenever a privileged-mode header is present never matches, and the presence assertion is silently skipped. An unauthenticated remote client can therefore send the header that activates a privileged branch while omitting the header the dependency was meant to require, bypassing the conditional check. Users should upgrade to fastify 5.12.2 or later.	7.5	More Details
CVE-2026-19080	Observable response discrepancy vulnerability in Menulux Software Inc. Menulux Portal allows Account Footprinting. This issue affects Menulux Portal: before 20260903211448.	7.5	More Details
CVE-2026-85581	SiYuan before v3.8.2 contains a denial of service vulnerability in the unauthenticated /api/system/uiproc endpoint that accepts and retains attacker-controlled process identifiers without size limits or authentication. Attackers can send repeated requests with unique identifiers to exhaust process memory and degrade service availability.	7.5	More Details
CVE-2026-86435	commonmark versions from 1.5.0 before 2.8.4 contain a denial of service vulnerability in the Footnote extension that fails to deduplicate footnote definitions. Attackers can craft documents with duplicate footnote definitions and references to create quadratic output expansion, consuming excessive memory and CPU to exhaust server resources.	7.5	More Details

CVE-2026-78480	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.5	More Details
CVE-2026-6377	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Next4Biz Information Technologies Inc. CSM (Customer Service Management) allows Path Traversal. This issue affects CSM (Customer Service Management): from 6.8.9 before 8.0.3.	7.5	More Details
CVE-2026-18453	A flaw was found in 389 Directory Server. A missing NULL pointer check in the paged results handling of op_shared_search allows an unauthenticated remote attacker to crash the LDAP server by sending a crafted sequence of search requests using the USE_ONE_BACKEND control, resulting in denial of service.	7.5	More Details
CVE-2026-14444	The WP Fusion (Pro) plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.47.13. This is due to insufficient authorization checks on the role parameter in the ThriveCart Auto Login handler's thrivecart() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, and who possess the access_key, to create a new user account with administrator privileges and gain full control over the WordPress site. The required access_key is intentionally shared with ThriveCart customers as part of the plugin's documented setup process, making it accessible to attackers who have made a purchase. The vulnerability is only exploitable when the ThriveCart Auto Login option is enabled.	7.5	More Details
CVE-2026-76560	A flaw was found in 389 Directory Server. The SELFDN ACI bind-rule evaluator incorrectly matches an anonymous LDAP client's empty bind DN against an empty stored attribute value, allowing an unauthenticated client to satisfy access control checks intended to require a matching authenticated identity. This can allow an anonymous LDAP client to perform an operation, such as adding or modifying a directory entry, that a SELFDN-based ACI intended to restrict to a specific authenticated user.	7.5	More Details
CVE-2026-85584	SiYuan versions before v3.8.2 contain a denial of service vulnerability in the publish-service Basic Auth throttle that stores failed-attempt state using attacker-controlled usernames without enforcing capacity limits or eviction policies. Unauthenticated attackers can submit repeated authentication requests with unique invalid usernames to exhaust memory and increase synchronization overhead, degrading service availability.	7.5	More Details
CVE-2026-85585	SiYuan before v3.8.2 contains an unbounded resource consumption vulnerability in the request-concurrency middleware that retains mutex entries for every unique request path without eviction. Unauthenticated attackers can send numerous unique request paths to permanently increase process memory and synchronization overhead, degrading availability.	7.5	More Details
CVE-2026-85450	MOOS core-moos through 10.4.0 contains a denial of service vulnerability in the MOOSDB HTTP server that creates unbounded connections and threads without limits. Attackers can open many connections and send endless header data to exhaust server threads and memory, causing service unavailability.	7.5	More Details
CVE-2026-85448	MOOS-IvP uFldShoreBroker through 24.8.1 fails to limit the number of claimed communities stored in parallel vectors within ShoreBroker::handleMailNodePing(). A single publisher can supply unbounded distinct community names to grow retained state and per-pass work without limit, causing memory exhaustion and performance degradation.	7.5	More Details
CVE-2026-81790	Missing Authorization vulnerability in Viszt Péter Csomagpontok és szállítási címkék WooCommerce-hez allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Csomagpontok és szállítási címkék WooCommerce-hez: from n/a before 4.2.8.	7.5	More Details
CVE-2026-85447	MOOS-IvP pRealm through version 24.8.1 accepts unbounded REALMCAST_REQ subscriptions without validating duration or variable list limits. Attackers can register long-lived pipeways with many variables to cause pRealm to generate excessive output indefinitely, exhausting system resources.	7.5	More Details
CVE-2026-18355	A heap buffer overflow flaw was found in the SASL I/O layer of 389 Directory Server (389-ds-base). In sasl_io_start_packet(), the wrapped-record length read from the wire is validated only against an upper bound. A small wire length (0, 1, or 2) produces an encrypted_buffer_count below the already-consumed encrypted_buffer_offset, causing an unsigned subtraction underflow in sasl_io_read_packet(). PR_Recv is then requested to read approximately 4 GiB into a 1024-byte heap buffer, resulting in a heap buffer overflow with attacker-controlled content. After a successful SASL bind with integrity protection (SSF > 0), a remote authenticated attacker can cause a denial of service or potentially achieve remote code execution. This flaw is distinct from CVE-2026-11774, whose fix only guards against upper-bound overflow.	7.5	More Details
CVE-2026-77465	toml-node is a TOML parser for Node.js and the browser. Prior to 4.2.0, toml.parse() uses a Peggy 5.1.0 generated recursive-descent parser in lib/parser.js whose peg$parsevalue, peg$parsearray, and peg$parseinline_table_entry functions recurse through nested arrays and inline tables without a depth limit. A remote unauthenticated application parsing an attacker-controlled TOML document containing a few thousand nested arrays or inline tables can exhaust the Node.js call stack, raise an unexpected RangeError rather than the parser's SyntaxError, and terminate an unprotected request worker or process. The corresponding grammar source is src/toml.pegjs, where the generated parser must be bounded. This issue is fixed in version 4.2.0.	7.5	More Details
	parsedmarc before 11.0.1 decompresses gzip and ZIP attachments in a single unbounded read with no limit		

CVE-2026-82520	on decompressed output size. Because parsedmarc automatically processes incoming DMARC report emails without user interaction, an unauthenticated remote attacker can send a crafted email with a highly compressed attachment to the monitored mailbox, causing the parsedmarc process to allocate memory proportional to the uncompressed size and exhaust available RAM.	7.5	More Details
CVE-2026-8862	IBM Netezza Software 11.3.0.3 through Interim Fix 002 has credentials that are hardcoded in the application source code, allowing unauthorized access to the container registry. The exposed secret enables attackers to pull private container images, potentially revealing proprietary code, configuration details, and other sensitive information.	7.5	More Details
CVE-2022-51009	PocketMine-MP before 4.7.2 fails to properly handle exceptions from the adhocore/json-comment library when parsing skin geometry data. Attackers can send login or skin packets with invalid geometry JSON to trigger an unhandled RuntimeException, causing server crash.	7.5	More Details
CVE-2026-86250	h3 versions before 2.0.1-rc.18 fail to validate the chunk count parsed from user-controlled cookie values in setChunkedCookie() and deleteChunkedCookie() functions. Attackers can send a crafted cookie header with an extremely large chunk count to trigger an O(n²) cleanup loop that hangs the server process.	7.5	More Details
CVE-2026-86259	OpenMAIC before 1.0.1 skips server-side request forgery validation in non-production builds, allowing unauthenticated attackers to reach cloud instance metadata services. Attackers can supply arbitrary provider URLs via the x-base-url header or baseUrl parameter to access sensitive cloud credentials and metadata.	7.5	More Details
CVE-2026-80229	When performing transfers via libcurl’s multi interface, pooled TLS connections can outlive their originating easy handles. In OpenSSL 3 provider configurations, libcurl attaches an allocated library context to the easy handle's state and passes it to OpenSSL without acquiring an ownership reference; destroying the easy handle prematurely frees this context while the active connection retains a dangling pointer, leading to a heap-use-after-free upon subsequent I/O or post-handshake operations.	7.5	More Details
CVE-2026-80230	When `CURLOPT_PINNEDPUBLICKEY` is configured alongside options that disable standard peer verification (`CURLOPT_SSL_VERIFYPEER = 0` and `CURLOPT_SSL_VERIFYHOST = 0`), libcurl fails to enforce public key pinning on connections established without a presented server certificate. Bypassing the pinning check under these disabled-verification conditions allows unauthenticated connections to succeed when they should be rejected.	7.5	More Details
CVE-2026-80231	A flaw in libcurl makes it wrongly reuse an existing HTTPS connection setup for a given hostname even when using a different Native CA Store setting (`CURLSSLOPT_NATIVE_CA`) than when the connection was created.	7.5	More Details
CVE-2026-80255	A `Set-Cookie:` header using tab (horizontal tab, ASCII code 9) instead of space (ascii code 32) immediately before the `Secure` attribute causes curl to store the cookie without its Secure flag. The cookie might then wrongfully be sent over plaintext HTTP on subsequent requests to the same host.	7.5	More Details
CVE-2026-85619	AppFlowy-Cloud 0.9.64 fails to verify that requested collab objects belong to the workspace in authorization checks, allowing attackers to access documents and database rows across workspaces. Attackers can supply a victim's object ID with their own workspace ID to bypass access controls and read, modify, or delete cross-workspace data.	7.5	More Details
CVE-2026-82208	With the wolfSSL backend, when CA caching is enabled and an `CURLOPT_SSL_CTX_FUNCTION` callback replaces the trust store, libcurl can silently reinstall the cached store after the callback returns. A certificate trusted by the cached store but rejected by the callback-selected store is then incorrectly accepted.	7.5	More Details
CVE-2026-14296	When using the Direct XIP update strategy, the main application image starts other cores (i.e. radio core), based on the currently active slot without additional verification. The MCUboot in the bare (upstream) configuration assumes that if there is at least a single slot for each image available, the system is bootable and continues the boot process. This may lead to a situation when MCUboot picks different slot for different images (i.e. (a) for the main application and (b) for the radio image), boots the main application (from slot (a)) that afterwards starts the radio image by providing an address of the unauthenticated slot ((a) instead of (b)).	7.5	More Details
CVE-2026-85608	Douyin_TikTok_Download_API through 4.1.2 contains a server-side request forgery vulnerability in the /api/download and /api/hybrid/video_data endpoints that allows unauthenticated attackers to fetch arbitrary URLs by supplying a url query parameter. Attackers can request internal services including cloud metadata endpoints and retrieve response bodies containing sensitive credentials through error messages.	7.5	More Details
CVE-2026-85429	MOOS-IvP uFldNodeComms through 24.8.1 trusts the source node identity from the message body rather than validating it from the connection source. Attackers can craft NODE_MESSAGE packets with spoofed source identities to impersonate other nodes and post arbitrary variable notifications without validation.	7.5	More Details
CVE-2026-86538	knowns versions before 0.30.0 contain a path traversal vulnerability in the POST /api/templates/preview endpoint that allows unauthenticated attackers to read arbitrary files. Attackers can supply directory traversal sequences in the templateFile parameter to bypass path restrictions and read sensitive files like credentials and configuration through the JSON response.	7.5	More Details

CVE-2026-85431	MOOS essential-moos through version 10.0.1 contains an unauthenticated UDP packet injection vulnerability in pMOOSBridge when configured with UDPListen. Attackers can send crafted UDP packets to the configured port to inject arbitrary variables into the local MOOS community with spoofed source and community identifiers.	7.5	More Details
CVE-2022-51017	PocketMine-MP versions before 3.26.5 and 4.0.5 fail to validate the length of skin data fields submitted by players, allowing uncapped values to exceed the 32767 byte TAG_String limit. Attackers can submit oversized skin data fields like skinID or geometryName to trigger exceptions during NBT data serialization, causing server crashes.	7.5	More Details
CVE-2026-85436	MOOS essential-moos through 10.0.1 contains a buffer overflow vulnerability in CMOOSUDPLink::ReadPktFromArray() that allows remote attackers to corrupt heap memory by sending UDP datagrams with negative declared lengths. Attackers can send crafted UDP packets to the configured UDPListen port to trigger an oversized memcpy operation that writes past the destination buffer, causing heap corruption and denial of service.	7.5	More Details
CVE-2026-85606	firecrawl-mcp-server 3.20.2 contains an arbitrary local file read vulnerability in the firecrawl_parse tool that accepts unconstrained filePath arguments without directory containment validation. Attackers can supply absolute paths or directory traversal sequences to read sensitive files like credentials and environment variables, which are then uploaded and returned to the model context.	7.5	More Details
CVE-2026-85441	MOOS core-moos through 10.4.0 fails to validate that serialized string lengths are non-negative in CMOOSMsg::operator>>. Unauthenticated attackers can send a crafted message with a negative length value to the MOOSDB port, causing an unhandled exception that terminates the database process.	7.5	More Details
CVE-2026-85442	MOOS core-moos through 10.4.0 fails to validate packet length declarations in CMOOSCommPkt::OnBytesWritten(), allowing unauthenticated attackers to trigger unbounded buffer allocation by sending crafted wire packets. Attackers can send packets with large declared lengths to exhaust server memory and cause denial of service before client authentication completes.	7.5	More Details
CVE-2026-85443	MOOS core-moos through 10.4.0 contains a denial of service vulnerability in MOOSCommServer::ListenLoop() where the accept thread performs a blocking receive without timeout during the wire-protocol handshake. An attacker can open a TCP connection to the MOOSDB port and send no data, causing the accept thread to block indefinitely while holding the socket-list lock, preventing all subsequent client connections.	7.5	More Details
CVE-2026-85444	MOOS-IvP through 24.8.1 contains a buffer over-read vulnerability in isQuoted(), isBraced(), and isChevroned() functions that strip whitespace but index using the original string length. Attackers can send NODE_REPORT messages with leading or trailing whitespace to read past buffer bounds and access adjacent memory.	7.5	More Details
CVE-2026-85445	MOOS-IvP through 24.8.1 contains a denial of service vulnerability in the Demuxer::addMuxPacket() function that trusts the packet count declared in mux headers without validation. Attackers can declare arbitrarily large packet counts to trigger unbounded memory allocation, exhausting system resources and causing service unavailability.	7.5	More Details
CVE-2026-85446	MOOS-IvP versions through 24.8.1 contain a quadratic processing vulnerability in uFldNodeComms where each new node identity creates a ledger entry and triggers all-pairs distribution work. Attackers can supply unbounded distinct node names in reports to drive the shoreside broker into quadratic processing, delaying or preventing distribution of legitimate node reports.	7.5	More Details
CVE-2026-76169	fastify versions >= 4.0.0 and before 5.12.2 can route a malformed URL sent under one plugin prefix to the custom not-found handler of a different sibling plugin, and invoke it without the preHandler hook declared for that handler. The internal not-found router for encapsulated handlers dispatches malformed paths through a single shared handler pointer before URL decoding, ignoring the prefix and skipping the selected handler's normal lifecycle. An unauthenticated attacker can therefore reach an authentication-protected private fallback through an unrelated public prefix and read its full response, bypassing the authentication hook and breaking prefix encapsulation. Users should upgrade to fastify 5.12.2 or later.	7.5	More Details
CVE-2026-81928	Net::DNS versions before 1.57 for Perl allow memory exhaustion via unbounded recursion in sig_data when re-encoding a message with a misplaced TSIG record. sig_data signs a message by re-encoding it, and removes TSIG records only from the additional section. A TSIG decoded into the answer or authority section survives that step and is signed again, so encoding re-enters sig_data with no termination condition. Decoding does not reject such a message: a TSIG that is not the last record on the wire raises "misplaced or corrupt TSIG", but the error is caught, reported as a warning, and the record is left in the packet. RFC 8945 section 5.2 requires the message to be dropped. The recursion is reached only when the decoded TSIG carries an empty MAC, since a MAC recovered from the wire short-circuits the signing step. It is reached only from code that re-encodes a message it decoded, such as a forwarder or a proxy. A decoded message that is never re-encoded is unaffected. Message direction does not matter: a query reaches the same path as a response. Each cycle re-encodes the whole message, so fewer than 100 bytes on the wire exhaust available memory and terminate the process.	7.5	More Details
	In FIPS mode, Libreswan's add_decoded_cert() function calls CERT_ExtractPublicKey() and asserts that the result is not NULL. However, CERT_ExtractPublicKey() returns NULL when public key extraction fails, for		

CVE-2026-14957	example if the RSA exponent is set to 0. A remote attacker can send a malformed X.509 certificate in a CERT payload to trigger the assertion, causing the pluto daemon to abort and restart. Continued exploitation causes a denial of service. No remote code execution is possible. Both IKEv1 and IKEv2 are affected. The vulnerability is only exploitable when both the OS and libreswan are running in FIPS mode and at least one CA certificate is loaded. The CERT payload is processed before peer authentication, so no credentials are needed to exploit this. Configurations using only PreSharedKey (PSK) authentication with no CA certificates loaded in the NSS database are not vulnerable.	7.5	More Details
CVE-2026-84382	HTTPX2 is a next generation HTTP client for Python. Prior to 2.12.0, the HTTPX2 content decoders in src/httpx2/httpx2/_decoders.py fully inflate each gzip, deflate, br, or zstd network chunk before iter_bytes() or aiter_bytes() yields bounded pieces to the application. A 64 KiB compressed chunk can expand to approximately 64 MiB in one intermediate allocation, so an attacker-controlled or compromised server can cause severe memory pressure or out-of-memory process termination even when the application streams the response. This issue is fixed in version 2.12.0.	7.5	More Details
CVE-2026-84484	ION-DTN versions before 4.2.0 contain an out-of-bounds read vulnerability in the decodeSdnv function that allows unauthenticated remote attackers to read memory by sending truncated SDNV values. Attackers can send a UDP datagram to the LTP link service input port with a truncated SDNV to trigger reads up to nine bytes past buffer boundaries and underflow byte counters.	7.5	More Details
CVE-2026-78662	Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.	7.5	More Details
CVE-2026-81774	Unauthenticated Sensitive Data Exposure in WooCommerce Product Attachment <= 2.3.3 versions.	7.5	More Details
CVE-2026-77792	The RegistrationMagic WordPress plugin before 6.0.9.9 does not escape a registration form field value before outputting it in an HTML attribute on an administrative page, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against high privilege users such as admin.	7.5	More Details
CVE-2026-78222	A vulnerability exists in NGINX JavaScript where a malformed HTTP response received by ngx.fetch() can crash an NGINX worker when trusted JavaScript reads Response.statusText. Exploitation requires control or influence over the fetched HTTP response. Impact: This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2026-18058	The mobile Smart Connect dashboard UI was subject to manipulation by 3rd party apps. When paired with a phishing attack, this manipulation could result in escalated privileges of an attacker within the system.	7.5	More Details
CVE-2026-84485	APITable through 1.13.0-beta.1 exposes the internal organization loadOrSearch endpoint without authentication, allowing unauthenticated attackers to retrieve member names, email addresses, and team hierarchy. Attackers can query the endpoint with space identifiers obtained from shared links or public templates to enumerate the complete member directory of any workspace.	7.5	More Details
CVE-2026-18672	In Progress® Telerik® UI for AJAX prior to v2026.3.812, insufficient validation of client-supplied state in RadImageEditor may allow an attacker to influence which file is returned by the control's image cache, potentially exposing file contents outside the intended image directories.	7.5	More Details
CVE-2026-84292	fast-uri serializes the port component of a URI without validating it. When recomposing the authority, the userinfo and host components are escaped but the port is concatenated verbatim, so a port value that is not a sequence of digits can inject authority delimiters, demoting the intended host to userinfo and pointing the authority at an attacker-controlled host. Both fast-uri and Node's URL read the result back as the attacker's host with no error, so re-validating the built URI does not catch it. This affects applications that build URIs from parts and assign untrusted data to the port component through the serialize, normalize, or equal functions in their object forms. The issue affects fast-uri versions before 2.4.6, from 3.0.0 before 3.1.7, and from 4.0.0 before 4.1.4. It is fixed in 2.4.6, 3.1.7, and 4.1.4, where recomposeAuthority rejects any port that is not a digit sequence per RFC 3986.	7.5	More Details
CVE-2026-84394	fast-uri accepts a host that contains an unbalanced or misplaced authority bracket without reporting an error. A host that starts with an opening bracket but does not end with a closing bracket is neither validated as an IP literal nor canonicalized as a domain name, so parse() returns it as the host with error undefined, while Node's URL and the HTTP clients built on it resolve the same string to a different host. An application that reads the parsed host to make a host decision, such as an SSRF denylist, a redirect allowlist, or proxy routing, and then passes the original URL to an HTTP client evaluates its policy against a string that is not the host the request reaches. The same host is carried through normalize, equal, and resolve. This affects fast-uri versions 2.4.5, 3.1.6, and 4.1.3, and is fixed in 2.4.6, 3.1.7, and 4.1.4, where parse() reports a malformed host for any host that contains a bracket but is not a valid IPv6 literal.	7.5	More Details

CVE-2026-84702	facefusion through 3.6.1 fails to normalize job identifiers in get_job_file_name, allowing attackers to write files outside the jobs directory. Attackers can supply traversal sequences in the job identifier parameter through the unauthenticated HTTP API to create files at arbitrary locations.	7.5	More Details
CVE-2026-56855	Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.	7.5	More Details
CVE-2026-84851	An uncontrolled recursion issue exists in Amazon Ion-C versions before 1.1.6 that might allow a remote unauthenticated actor to craft Ion data that exhausts the native call stack and crashes the application using the library, resulting in a denial of service.	7.5	More Details
CVE-2026-20281	A vulnerability in Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 that are running Cisco Session Initiation Protocol (SIP) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management when an affected device processes HTTP packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted HTTP packets to the device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, resulting in a DoS condition. A manual reboot of the device is required to recover from this condition. Note: For this vulnerability to be exploitable, the phone must be registered to Cisco Unified Communications Manager (Unified CM) and have Web Access enabled. Web Access is disabled by default.	7.5	More Details
CVE-2026-86098	ntop nDPI versions before 6.0 contain a heap buffer overflow vulnerability in the ndpi_json_string_escape function that writes beyond caller-supplied buffer boundaries. Attackers can trigger the overflow by supplying crafted network packet data including TLS SNI, HTTP headers, or DNS names that reach the vulnerable function, causing heap corruption.	7.4	More Details
CVE-2026-33388	An access control vulnerability was discovered in the Credentials Manager functionality due to insufficient validation of user privileges. A remote authenticated user with limited privileges can view a limited subset of the available entries in the Credentials Manager. The actual credential values are not directly visible, but the user can delete entries or edit their properties. An attacker who deletes or edits an entry can disrupt authentication for dependent devices, and one who manipulates an entry's configuration may be able to indirectly obtain the credentials.	7.4	More Details
CVE-2026-84777	Unauthenticated Broken Authentication in Really Simple SSL <= 9.8.0 versions.	7.4	More Details
CVE-2026-85525	Improper OCSP response validation in the Snowflake Python, Go, JDBC, and Node.js drivers allowed a revoked TLS certificate to be accepted as valid, because OCSP responses were not reliably bound to the certificate being validated and definitive verification failures were treated as transient. A man-in-the-middle attacker holding a revoked certificate and its private key for a Snowflake or stage hostname could cause the driver to establish a TLS session to the attacker-controlled endpoint anyway, allowing the attacker to read and modify data transmitted within that connection. Successful exploitation requires that on-path position and the corresponding private key, and impact is limited to data carried within the intercepted connection. The fix is available in the patched versions listed above. Users must manually upgrade.	7.4	More Details
CVE-2026-80131	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to remote execution.	7.4	More Details
CVE-2026-62906	Improper neutralization of special elements in data query logic in Microsoft Discovery Studio allows an unauthorized attacker to disclose information over a network.	7.4	More Details
CVE-2026-80164	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.4	More Details
CVE-2023-20577	A heap overflow in SMM module may allow an attacker with access to a second vulnerability that enables writing to SPI flash, potentially resulting in arbitrary code execution.	7.4	More Details
CVE-2026-79644	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.4	More Details
	undici 8.10.0 omits the destination origin from the cache and request-deduplication keys when the cache or deduplicate interceptor is composed directly onto a Client or Pool. Because the internal cache key falls back to an empty origin string, a cacheable or in-flight response from one upstream origin is returned for a request		

CVE-2026-85152	to a different, trusted origin whenever the method, path, and relevant headers match, which permits cross-origin information disclosure and persistent cache poisoning. The reporter demonstrated a full authentication bypass in which a JWT signed with an attacker-controlled key was accepted as belonging to a trusted issuer, and the trusted origin was never contacted. This is a regression introduced in 8.10.0 and affects undici versions from 8.10.0 up to 8.10.2. Applications using an Agent, which carries the origin in its dispatch options, are not affected. Users should upgrade to undici 8.10.2.	7.4	More Details
CVE-2026-84961	undici's BalancedPool constructor passes its entire options object through an internal deep-clone that serializes and reparses the value as JSON. Because JSON cannot represent functions, any function-valued TLS option, such as a caller-supplied checkServerIdentity callback or a custom connector inside the connect option, is silently discarded before it reaches the TLS layer. As a result a peer whose certificate the application's custom checkServerIdentity was written to reject, but which still passes Node's default hostname and chain checks, is accepted when reached through BalancedPool. The Client, Pool, and Agent dispatchers are not affected because they extract the connect and tls options before cloning. This affects undici versions from 7.24.1 up to 7.29.1 and from 8.0.0 up to 8.10.2, and only when the application supplies a function-valued connect or tls option to BalancedPool. Users should upgrade to undici 7.29.1 or 8.10.2.	7.4	More Details
CVE-2026-18489	IBM ContextForge MCP Gateway - Translate utility <= 1.0.8 MCP Context Forge could allow a remote attacker to obtain sensitive information from other sessions due to exposure of data elements to the wrong session.	7.4	More Details
CVE-2026-71375	Improper restriction of XML external entity reference vulnerability in Cosminexus Component Container. This issue affects Cosminexus Component Container: from 11-70-01 before 11-70-03, from 11-60 before 11-60-03, from 11-50 through 11-50-03, from 11-40 through 11-40-03, from 11-30 through 11-30-08, from 11-20 before 11-20-10, from 11-10 through 11-10-11, from 11-00 before 11-00-13, from 09-87 before 09-87-10, from 09-80 before 09-80-05, from 09-70 before 09-70-28, from 09-50 through 09-50-22, and from 09-00 through 09-00-18.	7.4	More Details
CVE-2026-75034	A flaw was found in Rancher Manager. The SAML assertion replay protection introduced by the fix for CVE-2026-44946 recorded consumed assertion IDs in a per-process cache, so each replica only detected replays that reached the same pod. In a high-availability deployment, an attacker holding a captured assertion could replay it once against every other replica to obtain additional authenticated sessions as the victim. This issue affects Rancher: before 2.15.1.	7.4	More Details
CVE-2026-84675	OS command injection vulnerability in Jenkins TICS Plugin 2025.1.1 and earlier allows attackers able to control build environment variable values to execute arbitrary commands on the agent running the build.	7.4	More Details
CVE-2026-62646	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). A session identifier is generated using an algorithm with insufficient randomness, resulting in a token with low entropy that can be predicted or brute-forced within a feasible number of attempts. This could allow an unauthenticated remote attacker to derive valid session identifiers and bypass authentication.	7.4	More Details
CVE-2026-62647	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). A random number generator is used to generate security-relevant values (such as session identifiers used for authentication purposes) that is not initialized with a True Random Number Generator (TRNG), resulting in a predictable sequence of generated values. This could allow an unauthenticated remote attacker to more easily predict the generated values and impersonate a legitimate authenticated user, potentially gaining unauthorized access to the device.	7.4	More Details
CVE-2026-73312	XenForo before 2.3.13 contains a refresh token replay vulnerability that allows attackers to reuse a refresh token multiple times by exploiting the failure to mark tokens as consumed when the parent access token has expired. Attackers can repeatedly submit the same refresh token to generate additional independent token pairs, achieving persistent unauthorized access for the token's full lifetime.	7.4	More Details
CVE-2026-73311	XenForo before 2.3.13 contains an OAuth2 authorization code reuse vulnerability that allows attackers to obtain unauthorized token pairs by submitting a previously used authorization code. Attackers can exploit the failure to invalidate or mark authorization codes as consumed after initial token issuance to receive an independent token pair for the same user and scopes, bypassing the single-use guarantee of the OAuth2 authorization code flow.	7.4	More Details
CVE-2026-86711	electerm before 5.3.15 exposes 40+ main-process functions through an unvalidated Electron IPC handler with no function-name allowlist or sender validation. Renderer-side script execution can invoke openFileWithEditor and other functions with arbitrary arguments to execute system commands in the main process.	7.4	More Details
CVE-2026-73309	XenForo before 2.3.13 contains an authentication bypass vulnerability in the OAuth2 token endpoint that allows unauthenticated attackers to obtain valid token pairs by submitting empty values for client_secret and code_verifier parameters. Attackers can exploit PHP truthy evaluation logic, which treats empty strings as false and skips client secret validation and PKCE code verifier validation, to exchange a valid authorization code for a token pair without proving client identity or holding the PKCE commitment.	7.4	More Details

CVE-2026-13608	A flaw in the libcurl SASL negotiation for LDAP authentication allows an incomplete handshake sequence to be misinterpreted as a successful cryptographic verification. An attacker executing a Man-in-the-Middle (MITM) attack can inject a premature or shortcut response that bypasses complete peer validation.	7.4	More Details
CVE-2026-86729	WWBN AVideo through commit e01e41ecc (no patched version available) exposes get_api_preauthorize in plugin/API/API.php as a second, undocumented login path. Unlike get_api_signIn, which enforces a rate limit of 10 attempts per 5 minutes via checkRateLimit(), get_api_preauthorize performs the same credential check with no throttling for any client, allowing unlimited remote password guessing against arbitrary accounts, including admin. The endpoint also acts as a credential oracle: it returns the message "Invalid credentials" for both correct and incorrect passwords, while the users_id field in the response body discloses the authenticated identity (users_id:1 on success, users_id:0 on failure), and a correct password establishes a session cookie that remains usable for authenticated API requests. Together these issues permit unauthenticated brute-force account takeover.	7.4	More Details
CVE-2026-80133	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Relative Path Traversal vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to remote execution.	7.4	More Details
CVE-2026-78254	The ftp and scp tasks of Apache Ant can download files from a remote server. A malicious server can provide relative paths that allow it to write outside of the dedicated target directory for the download, making it possible to overwrite files of the attacker's choice using the permissions of the user running Ant in versions prior to Ant 1.10.18. In order to exploit this vulnerability, the server would either have to be malicious or be subject to a machine-in-the-middle attack. Additionally in the case of scp or the ftp task using ftps the server must pass the server identity checks performed by the tasks. For ftp tasks not using ftps a malicious server could act as a machine-in-the-middle to provide malicious files. Starting with Ant 1.10.18 both tasks will prevent writing outside of the destination directory by default. An option is available to disable this behavior in the unlikely case that the old behavior is required by existing build files. Mitigations: Users of scp and ftp (when using ftps) in any version of Ant should not bypass server identity checks. Users of ftp not using ftps should switch to ftps where possible. All users are recommended to upgrade to Apache Ant 1.10.18, which fixes this issue.	7.4	More Details
CVE-2026-85091	zlib versions 1.3.1.2 through 1.3.2 contain a heap buffer overflow vulnerability in the gz_vacate() function when processing non-blocking gzwrite() operations with stale external buffer pointers. Attackers can trigger the overflow by calling gzprintf() or gzvprintf() after a write stall, causing an unchecked memmove() to write beyond the internal input buffer boundary.	7.4	More Details
CVE-2026-86306	A weakness has been identified in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. This affects an unknown part of the file App/Home/Model/UserModel.class.php of the component Cookie Helper. Executing a manipulation of the argument Username can lead to improper authentication. 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.	7.3	More Details
CVE-2026-86666	A security flaw has been discovered in aircheng-org iWebShop-5 up to 5.15. Impacted is the function upload_json/uploadFile of the file controllers/pic.php. The manipulation results in unrestricted upload. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-86277	A vulnerability has been found in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. Impacted is an unknown function of the file delete_exam.php. The manipulation of the argument ID leads to authorization bypass. 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-2026-86276	A flaw has been found in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. This issue affects some unknown processing of the file db.php. Executing a manipulation can lead to hard-coded credentials. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-85512	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0. This vulnerability affects unknown code of the file /admin/session.php. The manipulation of the argument ID results in missing authorization. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-79643	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Use of Incorrect Operator vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	7.3	More Details
CVE-2026-86220	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. The affected element is the function mysqli_query of the file /admin/modal_add_course.php. The manipulation of the argument course results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	7.3	More Details

CVE-2026-86273	A weakness has been identified in projeto-siga siga up to 11.1.1. Affected by this issue is the function DownloadExterno.getUrl of the file sigaex/src/main/java/br/gov/jfrj/siga/vraptor/ExUtilController.java of the component HTML-to-PDF Endpoint. This manipulation of the argument html causes server-side request forgery. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-86272	A vulnerability was determined in Beijing Meite Software Technology U+Smart Enjoyment WebSite 18.6001.1096.1000. This impacts an unknown function of the file /Report/Upload/UploadFormImg.ashx. Executing a manipulation of the argument File can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-86268	A vulnerability was detected in itsourcecode School Management System 1.0. Impacted is an unknown function of the file User_Login.php. The manipulation of the argument email results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-85638	A weakness has been identified in jofpin trape 2.0. This affects an unknown part of the file core/user.py. This manipulation of the argument vId/id causes authorization bypass. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-85105	A flaw has been found in NousResearch hermes-agent 0.18.0. Affected by this issue is the function _sess_nowait of the file s71.py of the component Session Management. This manipulation of the argument session_id causes authorization bypass. The attack can be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-86263	A vulnerability was detected in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. This impacts the function orderRecordsService.cancelOrder of the file ssm_pro/src/main/java/cn/sfturing/web/OrderController.java of the component Order Cancellation. The manipulation of the argument ID results in authorization bypass. The attack may be performed from remote. The exploit is now public and may 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-2026-80738	In the Linux kernel, the following vulnerability has been resolved: bpf: Check sk_state before sk_protocol in bpf_tcp_*_syncookie bpf_tcp_gen_syncookie and bpf_tcp_check_syncookie accept a socket pointer 'sk' with argument type ARG_PTR_TO_BTF_ID_SOCK_COMMON. However, they access sk->sk_protocol without validating whether 'sk' represents a full socket. Fix this issue by checking sk->sk_state != TCP_LISTEN before inspecting sk->sk_protocol in both bpf_tcp_gen_syncookie and bpf_tcp_check_syncookie. Since mini-sockets are never in the TCP_LISTEN state, the condition short-circuits and prevents dereferencing fullsock-specific fields.	7.3	More Details
CVE-2026-84441	A security vulnerability has been detected in Piwigo up to 16.3.0. Affected by this issue is some unknown functionality of the file i.php of the component Image Derivative Handler. The manipulation leads to path traversal. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-86282	A weakness has been identified in jaychouchannel Tourism-Management-System up to 8122bf020d91199eddfff3ee02d1632a70a9a132. Affected is an unknown function of the file travel/src/main/java/com/controller/CommonController.java of the component CommonDao. Executing a manipulation of the argument table/column/xColumn/yColumn can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. This patch is called d44ec3aa0bd2a72c8800e3befb0a9a96a6491b86. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2026-85702	A security vulnerability has been detected in ramon-victor freegpt-webui up to 098db3dfeb41555c2ca9269df0f13e10ec1c35dc. Affected is the function _conversation of the file server/backend.py of the component Backend Conversation API. Such manipulation of the argument model leads to missing authentication. The attack may be launched remotely. The exploit has been disclosed publicly and may 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. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-86305	A security flaw has been discovered in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. Affected by this issue is the function Upload::upload of the file ThinkPHP/Library/Think/Upload.class.php. Performing a manipulation results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. 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-2026-86303	A vulnerability was determined in 92181 markdown up to 058cab0cb7fb245a0ccc6b8446963ff8d573558f. Affected by this issue is the function lds of the file md.c. Executing a manipulation can lead to out-of-bounds read. The attack can be executed remotely. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. This patch is called c000d2f9cf390c315378d3717cf20911cf3e80a6. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2026-85516	A vulnerability was detected in code-projects Vehicle Management System 1.0. The affected element is an unknown function of the file /busprofile.php. Performing a manipulation of the argument busid results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-84652	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, Jenkins does not rotate the session when a user is authenticated via the "remember me" cookie, allowing attackers able to serve content on the same site as Jenkins to set a known session cookie in the victim's browser, which after the victim authenticates via the "remember me" cookie, grants the attacker access to Jenkins as that user.	7.3	More Details
CVE-2026-86290	A weakness has been identified in SourceCodester Online Voting System 1.0. This affects an unknown function of the file /voting/ajax.php?action=save_category. This manipulation of the argument Category causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-85208	A security flaw has been discovered in itsourcecode Online Medicine Delivery System 1.0. The affected element is the function doInsert of the file /rider/orders/controller.php?action=add of the component Order Management Controller. Performing a manipulation of the argument image results in unrestricted upload. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-86292	A vulnerability was detected in SourceCodester Simple Traffic Offense System 1.0. Affected is an unknown function of the file saveuser.php of the component User Creation. Performing a manipulation of the argument position results in missing authentication. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-78590	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) in the Kibana Fleet feature can lead to the unauthorized deletion of privileged resources via Path Traversal (CAPEC-126). A low-privileged user holding Fleet Settings write access could cause a subsequent administrative action to act on unintended internal resources, resulting in the deletion of privileged resources such as user accounts and other organizational assets. Exploitation requires an administrator to interact with the affected Fleet interface.	7.3	More Details
CVE-2026-85187	A security vulnerability has been detected in itsourcecode Online Medicine Delivery System 1.0. Affected by this issue is the function Order::pupdate of the file /rider/orders/controller.php?action=edit&actions=confirm of the component Order Status Update. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-86298	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0. Impacted is an unknown function of the file /delete_subject.php. Performing a manipulation of the argument ID 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.	7.3	More Details
CVE-2026-85137	A security vulnerability has been detected in SeaCMS up to 13.6. This impacts the function parseIf of the file seacms_locoy_news.php of the component Locoy Collector. The manipulation of the argument pwd leads to code injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-85138	A vulnerability was detected in SeaCMS up to 13.6. Affected is the function addslashes of the file weixin/index.php of the component WeChat Module. The manipulation of the argument Content results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-61409	Dell Secure Connect Gateway (SCG) 5.0 Application, versions prior to 5.36.00.00, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to remote execution.	7.3	More Details
CVE-2026-86300	A flaw has been found in Tenda AC9 15.03.05.14. This impacts the function R7WebsSecurityHandler of the component Web Management. This manipulation causes improper authentication. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-86221	A flaw has been found in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is the function mysqli_query of the file /admin/modal_add_course1.php. This manipulation of the argument course causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access	7.3	More Details

79691	could potentially exploit this vulnerability, leading to protection mechanism bypass.		
CVE-2026-80735	In the Linux kernel, the following vulnerability has been resolved: ovpn: ensure socket is owned by ovpn before deref sk_user_data Some subsystems, like BPF SOCKMAP, set sk_user_data without actually setting the encap_type. For this reason, we must make sure that the type is the one ovpn expects before dereferencing sk_user_data. Failing to do so may lead to out-of-bounds reads.	7.3	More Details
CVE-2026-86209	A weakness has been identified in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /delete_user.php. This manipulation of the argument ID 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-2026-86180	A vulnerability has been found in code-projects Task Management System In PHP 1.0. Affected by this vulnerability is an unknown functionality of the file /index.php of the component Login. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-86223	A vulnerability was found in SourceCodester Class and Exam Timetabling System 1.0. This impacts the function mysqli_query of the file /admin/modal_add_coursea.php. Performing a manipulation of the argument course results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-86168	A security flaw has been discovered in code-projects Content Management System 1.0. The affected element is an unknown function of the file /login.php. The manipulation of the argument user_name results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-86224	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. Affected is the function mysqli_query of the file /admin/modal_add_product.php. Executing a manipulation of the argument fname can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-86162	A vulnerability was determined in SourceCodester Online Voting System 1.0. This affects an unknown function of the file /ajax.php?action=login. Executing a manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-86161	A vulnerability was found in SourceCodester Online Voting System 1.0. The impacted element is an unknown function of the file /ajax.php?action=delete_category. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-86160	A vulnerability has been found in SourceCodester Online Voting System 1.0. The affected element is an unknown function of the file /ajax.php?action=delete_voting. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-86159	A flaw has been found in SourceCodester Online Voting System 1.0. Impacted is an unknown function of the file /ajax.php?action=save_user. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-86210	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /delete_user_account.php. Such manipulation of the argument ID 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-2026-86211	A flaw has been found in rabindralamsal inventory-management-system 1.0.0. This affects an unknown part of the file index.php of the component Login. Executing a manipulation of the argument username/password can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-86225	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is the function mysqli_query of the file /admin/modal_add_room.php. The manipulation of the argument room_name leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-86213	A vulnerability was found in Mstfakts College-Management-System. This issue affects the function mysqli_query of the file Front-end/university.php of the component Search Handler. The manipulation of the argument book_name/book_author results in sql injection. The attack may be performed from remote. The exploit has been made public and could 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-2026-84841	A security flaw has been discovered in tsi-coop tsi-dpdp-cms up to 0.5.0. This vulnerability affects unknown code. The manipulation results in client-side enforcement of server-side security. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.5.1 is able to resolve this issue. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2026-85225	A vulnerability was identified in code-projects Doctor Appointment System 1.0. This vulnerability affects unknown code of the file /patient_login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-86214	A vulnerability was determined in Mstfakts College-Management-System. Impacted is an unknown function of the file Front-end/login.php. This manipulation of the argument email causes improper authentication. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-85378	A vulnerability was identified in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. Affected by this issue is the function AuthController::_initialize of the file App/Admin/Controller/ChapterController.class.php of the component Chapter Controller. The manipulation leads to authorization bypass. The attack can be initiated remotely. The exploit is publicly available and might 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-2026-86261	A weakness has been identified in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. The impacted element is an unknown function of the file ssm_pro/src/main/java/cn/sfturing/web/OrderController.java of the component Order Controller. Executing a manipulation of the argument userIdenf can lead to authorization bypass. 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 project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-86665	A vulnerability was identified in aircheng-org iWebShop-5 up to 5.15. This issue affects the function Update::index of the file controllers/update.php. The manipulation leads to missing authorization. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-85379	A security flaw has been discovered in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. This affects the function ChapterModel::searchChapter of the file App/Home/Controller/ChapterController.class.php of the component Query Builder. The manipulation of the argument content results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. 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.	7.3	More Details
CVE-2026-85380	A weakness has been identified in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. This vulnerability affects the function catchimage of the file Public/ueditor/php/controller.php of the component UEditor. This manipulation of the argument source[] causes server-side request forgery. The attack may be initiated remotely. The exploit has been made available to the public and could 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-2026-85397	A vulnerability was determined in code-projects Hospital Information System 1.0. This impacts the function findBySearch of the file addReq.php. This manipulation of the argument Search 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-2026-85398	A vulnerability was identified in code-projects Hospital Information System 1.0. Affected is the function viewReq of the file viewReq.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-85399	A security flaw has been discovered in code-projects Hospital Information System 1.0. Affected by this vulnerability is the function getSinglePresp of the file includes/presp/PrespController.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-85402	A vulnerability was detected in code-projects Doctor Appointment System 1.0. This vulnerability affects unknown code of the file /patient/booking.php. The manipulation of the argument doc_id results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details

CVE-2026-86222	A vulnerability has been found in SourceCodester Class and Exam Timetabling System 1.0. This affects the function mysqli_query of the file /admin/modal_add_course2.php. Such manipulation of the argument course leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-85403	A flaw has been found in code-projects Doctor Appointment System 1.0. This issue affects some unknown processing of the file /contactus.php. This manipulation of the argument firstname causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	7.3	More Details
CVE-2026-76759	Vulnerability in Drupal Screenshot. This issue affects Screenshot versions: *.*.	7.3	More Details
CVE-2026-76782	Vulnerability in Drupal Screenshot. This issue affects Screenshot versions: *.*.	7.3	More Details
CVE-2026-86262	A security vulnerability has been detected in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. This affects the function updateOrderSta1/updateOrderdiseaseInfo of the file ssm_pro/src/main/java/cn/sfturing/web/OrderController.java of the component Order Handler. The manipulation of the argument userID/id leads to authorization bypass. The attack is possible to be carried out remotely. The exploit has been disclosed publicly 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.	7.3	More Details
CVE-2026-86208	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0. This impacts an unknown function of the file /delete_teacher.php. The manipulation of the argument ID 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-2026-82524	UnoPim before 2.1.5 contains an authenticated file upload vulnerability that allows authenticated administrators to upload arbitrary PHP files through the TinyMCE image upload endpoint due to missing file extension and MIME type validation. Attackers can upload a PHP web shell to the public storage disk and execute arbitrary operating system commands on the server by accessing the uploaded file at the URL returned in the server response.	7.2	More Details
CVE-2026-85599	Grav Shortcode Core before 6.2.5 contains stored cross-site scripting vulnerabilities in the [lorem] tag parameter and [details] summary parameter that are written to rendered pages without escaping. Attackers with page-edit access can inject arbitrary HTML and JavaScript that executes in the browsers of all page visitors, including administrators.	7.2	More Details
CVE-2026-74239	XenForo before 2.3.13 contains a path traversal vulnerability in the style archive importer on Windows deployments that allows authenticated non-super administrators with style permissions to write arbitrary files outside the intended extraction directory by using backslash-based traversal sequences in ZIP member names. Attackers can craft a malicious ZIP archive with backslash path separators that bypass forward-slash validation to write arbitrary bytes to any web-server-writable path, including the public web root, achieving persistent code execution as the web-server account.	7.2	More Details
CVE-2026-19224	The Hummingbird Performance WordPress plugin before 3.21.2 does not restrict a network-wide setting to network administrators, allowing an administrator of any single site on a multisite network to execute arbitrary code across the entire network.	7.2	More Details
CVE-2026-84761	Unauthenticated Server Side Request Forgery (SSRF) in LiteSpeed Cache <= 7.9 versions.	7.2	More Details
CVE-2026-84773	Unauthenticated Cross Site Scripting (XSS) in EWWW Image Optimizer <= 8.7.6 versions.	7.2	More Details
CVE-2026-61517	Netis NX10 firmware V4.0.1.5808 and V3.0.0.4142 contain an OS command injection vulnerability in the ping diagnostic handler that allows authenticated administrators to execute arbitrary shell commands as root by injecting into the IpAddr parameter. The parameter is interpolated directly into a shell command executed through system() with an incomplete denylist that only blocks spaces, pipes, semicolons, and ampersands, leaving command substitution and alternate field separator expansion available for exploitation.	7.2	More Details
CVE-2026-76561	A flaw was found in Dogtag PKI, as used by FreeIPA's certificate authority component. The certificate profile import functionality does not fully validate uploaded profile content beyond the profile ID. An authenticated user with CA Administrator privileges can exploit Dogtag's ExternalProcessConstraint mechanism to execute arbitrary commands with attacker-controlled environment variables, achieving code execution as the pkiuser	7.2	More Details

	account.		
CVE-2026-86437	Lara Dashboard before 1.3.2 authorizes the POST /admin/settings/core-upgrades/upload endpoint with only the settings.edit permission, allowing non-Superadmin administrators to upload and extract arbitrary zip archives over the live application source code. Attackers can upload a malicious archive containing modified application files such as routes/web.php with embedded system commands, which execute as the web server user with access to environment secrets and database credentials.	7.2	More Details
CVE-2026-86438	Lara Dashboard before 1.3.2 fails to authorize the MarketplaceModuleBrowser installModule Livewire action, allowing non-Superadmin administrators to install modules. Attackers can download and auto-activate arbitrary PHP modules from the marketplace over unsigned HTTP requests, achieving remote code execution.	7.2	More Details
CVE-2026-18406	The SureForms – Contact Form Builder, AI Forms, Payment Form, Survey & Quiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Text Field Entity-Encoded Payload in all versions up to, and including, 2.12.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-16649	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Post Body Field Value in all versions up to, and including, 2.10.5 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 exploit survives save-time sanitization because wp_kses_post allows the required HTML tags and attributes, and the client-side tooltip script re-parses the browser-decoded aria-label value as innerHTML while only stripping script elements, leaving onerror and other event-handler attributes fully intact and executable.	7.2	More Details
CVE-2026-15984	The QuickCal plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Custom Field Parameters in all versions up to, and including, 1.0.20 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 nonce guarding the unauthenticated booked_add_appt AJAX action is publicly embedded on any page rendering the booking calendar shortcode, making it trivially obtainable by unauthenticated attackers without any prior account or privilege.	7.2	More Details
CVE-2026-77263	The iubenda | All-in-one Compliance for GDPR / CCPA Cookie Consent + more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 3.13.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit works by embedding KSES-allowed markup such as abbr title attributes and HTML comments in a submitted comment so that the global strtr() substitution strips substrings from an inert tag, mutating it into an executable element such as an img onerror handler that runs in the WordPress origin for any visitor, including logged-in administrators.	7.2	More Details
CVE-2026-77233	The iubenda | All-in-one Compliance for GDPR / CCPA Cookie Consent + more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via AdSense Regex Rewrite in all versions up to, and including, 3.13.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability only manifests when the 'Secondary' parser engine is active (parser_engine=default); it does not exist under the default 'new' DOM-based parser engine.	7.2	More Details
CVE-2026-78438	The W3 Total Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via LazyLoad Background Mutator in all versions up to, and including, 2.10.5 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. This requires the "Lazy Load Images" feature with "Process background images" to be enabled, and the malicious comment to be approved by a moderator before execution is triggered.	7.2	More Details
CVE-2026-79426	An arbitrary file deletion vulnerability in the /adminapi/file/video_data_save component of CRMEB v6.0.0 allows authenticated attackers to delete arbitrary files via crafted POST request.	7.2	More Details
CVE-2026-83625	The Contact Form by Supsystic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via IP Address Header in all versions up to, and including, 1.10.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. An unauthenticated attacker can first call the 'updateNonce' action — which is accessible without authentication due to its absence from the plugin's permission list — to obtain a valid nonce, then submit a contact form with a malicious payload in a spoofed IP header such as X-Forwarded-For.	7.2	More Details
CVE-2026-86188	AVideo with YPTSocket plugin enabled contains a cross-site scripting vulnerability allowing unauthenticated attackers to execute arbitrary JavaScript in other users' browsers via the websocket callback mechanism. Attackers can send crafted socket messages with callback names resolving to global functions like avideoConfirmHTML that accept untrusted data and assign it to innerHTML, achieving script execution in the	7.2	More Details

	victim's origin without authentication or user interaction.		
CVE-2026-86431	league/commonmark (thephpleague/commonmark) versions >= 2.7.0 and < 2.9.1 contain a cross-site scripting vulnerability in the AttributesExtension. Prefixing an attribute name with a single U+000C form feed byte (e.g. {\x0Conclick="alert(1)"}) bypasses the AttributesHelper::filterAttributes() 'on*' event-handler filter because PHP's trim() does not strip U+000C, causing the attribute to be written verbatim into the output where browsers parse it as a genuine event handler. The same prefix also defeats the allow_unsafe_links check, allowing javascript: URIs through href/src attributes even when allow_unsafe_links is false. Exploitation requires processing untrusted Markdown with the AttributesExtension enabled; the injected script executes when the rendered HTML is viewed. Fixed in 2.9.1.	7.2	More Details
CVE-2026-75528	The Broken Link Checker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Author URL / Link Log in all versions up to, and including, 2.4.13 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 perform the plugin's standard dismiss-and-recheck workflow on a link submitted by the attacker via the WordPress comment author URL field, after which the attacker's HTTP server issues a redirect to a URL containing an HTML/JavaScript payload that is stored verbatim in the link log.	7.2	More Details
CVE-2026-80127	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to elevation of privileges.	7.2	More Details
CVE-2026-77830	The Spam protection, Honeypot, Anti-Spam by CleanTalk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content aria-label Placeholder in all versions up to, and including, 6.86 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. The payload is deliverable via unauthenticated comment submission and executes exclusively for non-logged-in visitors; if comment moderation is enabled, an approving moderator must first publish the comment before the script reaches other users.	7.2	More Details
CVE-2026-19769	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Repeater Child 'type' Confusion via Unmatched Array Key in all versions up to, and including, 3.15.1 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 the Ninja Forms File Uploads add-on to be active, as the attack routes the unwhitelisted child entry through the File Uploads handler to write an attacker-supplied HTML file containing arbitrary JavaScript into any web-server-writable directory, including the site root, where it is served from the site's own origin.	7.2	More Details
CVE-2026-86539	knowns through 0.33.0 contains a server-side request forgery vulnerability in the POST /api/embedding-models/test endpoint that issues outbound requests to caller-supplied destinations without validation. Attackers can enumerate internal hosts and cloud metadata endpoints by observing transport error messages that reveal network reachability information.	7.2	More Details
CVE-2026-81806	Server-Side Request Forgery (SSRF) vulnerability in John Darrel Hide My WP Ghost allows Server Side Request Forgery. This issue affects Hide My WP Ghost: from n/a through 7.0.09.	7.2	More Details
CVE-2026-6431	The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Biographical Info' meta field parameter in all versions up to, and including, 3.15.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-86733	Snipe-IT before 8.7.0 streams the SQL entry from an uploaded backup archive directly into the MySQL/MariaDB command-line client (`mysql`) without the --binary-mode flag, so the client interprets lines beginning with backslash commands such as `\!` as local shell commands. An authenticated superadministrator who uploads a crafted ZIP backup (POST /admin/backups/upload) and triggers a restore (POST /admin/backups/restore/{filename}) without the optional `clean` sanitizer parameter — which is not applied by default because DB_SANITIZE_BY_DEFAULT is false — can execute arbitrary OS commands as the web application's operating-system user, exposing application secrets (including database credentials and APP_KEY) and allowing modification of application-writable files and data. Version 8.7.0 adds the --binary-mode flag to the client invocation.	7.2	More Details
CVE-2026-84387	A improper neutralization of special elements used in a command ('command injection') vulnerability in Fortinet FortiSandbox 5.2.0, FortiSandbox 5.0.0 through 5.0.6, FortiSandbox 4.4.0 through 4.4.9 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	7.2	More Details
CVE-2026-	Unauthenticated Cross Site Scripting (XSS) in Estatik <= 4.3.4 versions.	7.1	More Details

81775			
CVE-2026-84800	Craft CMS versions >= 5.0.0-RC1 and < 5.10.11 contain a missing authorization vulnerability in AssetsController::actionReplaceFile. When a request supplies sourceAssetId and targetFilename but omits assetId, the target asset is resolved by folder and filename after the permission checks execute, so the replacePeerFiles permission is never enforced. An authenticated low-privilege author with only the replaceFiles permission on a shared folder can overwrite the content of a peer's asset file (located in the same folder) with attacker-controlled bytes. Fixed in 5.10.11.	7.1	More Details
CVE-2026-84759	Unauthenticated Cross Site Request Forgery (CSRF) in Activity Log <= 2.13.1 versions.	7.1	More Details
CVE-2026-81771	Unauthenticated Cross Site Scripting (XSS) in TrustedSite <= 1.2.5 versions.	7.1	More Details
CVE-2026-84798	Craft CMS versions >= 5.0.0-RC1 and < 5.10.11 fail to perform an independent authorization check in ElementsController::actionDeleteForSite(). The method loads an element with checkForProvisionalDraft enabled and runs the deletion authorization check against the user's own provisional draft (which only verifies draft ownership), then propagates the deletion to the canonical element without re-checking permissions. As a result, an authenticated user who has viewEntries, viewPeerEntries, saveEntries, savePeerEntries, and editSite permissions but lacks the deleteEntriesForSite permission can hard-delete a canonical entry's site record (and, for single-site entries, the full element and content), which is irrecoverable via Craft's recycle bin.	7.1	More Details
CVE-2026-81404	The IPGP Visitors Origin WordPress plugin before 1.6 does not sanitise or escape user input before reflecting it back in the HTTP response, allowing unauthenticated attackers to perform Reflected Cross-Site Scripting attacks against users who are tricked into submitting a crafted request.	7.1	More Details
CVE-2026-85451	MOOS core-moos through 10.4.0 contains a remote process termination vulnerability in the SuicidalSleeper component that uses a hard-coded passphrase for multicast command authorization. Any multicast-reachable peer can enumerate MOOS processes and send termination commands to trigger process shutdown by exploiting the default multicast group and port with the known passphrase.	7.1	More Details
CVE-2026-84794	Craft CMS versions before 5.10.11 lack authorization checks in the assets/move-asset endpoint when force=1 is supplied. Authenticated users without peer asset permissions can move their own assets into other users' folders and force deletion of conflicting files, allowing unauthorized asset deletion and replacement.	7.1	More Details
CVE-2026-86718	WWBN AVideo through commit c3edcc274c389816d434acadac07ee78eaf330c1 contains a cross-site request forgery vulnerability in deleteHistory.json.php and finishAll.json.php that allows unauthenticated attackers to mutate live history by making GET requests without CSRF token validation. Attackers can craft malicious pages that trigger administrator browsers to delete all live transmission history or mark streams as finished when an admin visits the attacker-controlled site.	7.1	More Details
CVE-2026-81770	Unauthenticated Cross Site Scripting (XSS) in Interactive Geo Maps <= 1.6.30 versions.	7.1	More Details
CVE-2026-81289	Unauthenticated Cross Site Scripting (XSS) in MP3 Audio Player for Music, Radio & Podcast by Sonaar <= 5.13.1 versions.	7.1	More Details
CVE-2026-81288	Unauthenticated Cross Site Scripting (XSS) in Upsell Order Bump Offer for WooCommerce <= 3.1.5 versions.	7.1	More Details
CVE-2026-53728	Medplum is a developer platform that enables development of healthcare apps. Prior to version 5.1.6, the external identity provider callback at GET /auth/external accepts attacker-controlled redirect URIs that only need to start with a registered client redirect URI, rather than matching exactly. After a successful external IdP login, the server appends Medplum login and code values to that attacker-supplied URL and issues a redirect. Because the external login request state is serialized as raw JSON and later trusted by the callback, an attacker who can tamper with state.redirectUri can cause Medplum to redirect authorization artifacts to an attacker-controlled endpoint. When the registered redirect URI is a bare origin or another prefix that can be extended into a different hostname, this becomes a cross-origin authorization code leak. This issue has been patched in version 5.1.6.	7.1	More Details
CVE-2026-86713	PX4 Autopilot through 1.17.0 contains a use-after-free vulnerability in the load_mon module's stop path where exit_and_cleanup() deletes the LoadMon object and frees the performance counter before perf_end() attempts to access it. Attackers can trigger this vulnerability by issuing the load_mon stop command from any PXH or MAVLink shell, causing reads and writes through freed memory that corrupt heap objects and destabilize the flight stack.	7.1	More Details

CVE-2026-16281	The Classified Listing WordPress plugin before 6.1.1 does not verify that the caller owns or can edit the target listing before its AI image-editing AJAX action deletes or attaches media, allowing any authenticated user, including a subscriber, to permanently delete attachments from, and attach files to, any listing owned by another user.	7.1	More Details
CVE-2026-12865	The Photo Gallery by 10Web WordPress plugin before 1.8.44 does not escape two request parameters before reflecting them into input-attribute values on its admin pages (one on the Shortcode page, one on the Galleries/Albums list page), so an unauthenticated attacker can craft a link that, when opened by a logged-in administrator (or, for the first sink, a contributor), executes arbitrary JavaScript in the victim's authenticated session via an auto-firing onfocus handler. The Galleries/Albums sink renders only when the site has more than 20 galleries/albums (the normal state of a populated install).	7.1	More Details
CVE-2026-84667	Jenkins ThinBackup Plugin 2.1.4 and earlier allows overwriting the plugin's backup configuration through Stapler data binding, allowing attackers to redirect backup writes to an attacker-specified directory and to include arbitrary files from the Jenkins controller file system in backups.	7.1	More Details
CVE-2026-9331	The EDD Product Catalog Feed by PixelYourSite plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the wpeddpcf_delete_feed function in all versions up to, and including, 1.0.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary option values on the WordPress site. This can be leveraged to delete an option that would create an error on the site and deny service to legitimate users.	7.1	More Details
CVE-2026-19453	The JetBackup WordPress plugin before 3.1.23.5 does not verify the role or capabilities of the account it preserves across a restore or migration before granting it administrator privileges, allowing a subscriber-level user to gain administrator access after the site owner restores or migrates the site.	7.1	More Details
CVE-2026-19723	The Social Media Share Buttons & Social Sharing Icons WordPress plugin before 3.0.1 does not properly escape a value taken from the incoming request before outputting it in an inline JavaScript event handler, leading to Reflected Cross-Site Scripting which is triggered when a user interacts with the affected button. Exploitation requires the Social Media Share Buttons & Social Sharing Icons WordPress plugin before 3.0.1 to be running a non-default icon display configuration.	7.1	More Details
CVE-2022-35499	In Trimble TM4WEB 21.4.0.4, the external bill viewer endpoint is vulnerable to reflected cross-site scripting via injection in a arbitrary parameter appended to the URL.	7.1	More Details
CVE-2026-14199	Only self-managed Grafana instances with Auth Proxy authentication and identity caching enabled (sync_ttl greater than zero) are affected. The Auth Proxy cache key concatenated the username and forwarded identity attributes without a delimiter, so distinct identities could collide on one key. An authenticated user who shapes their own attributes to collide with a higher-privileged user's, while that user's cache entry is live, is authenticated as that user, up to Administrator (authentication bypass by spoofing).	7.1	More Details
CVE-2026-84820	Unauthenticated Cross Site Scripting (XSS) in Unlimited Elements For Elementor (Free Widgets, Addons, Templates) <= 2.0.17 versions.	7.1	More Details
CVE-2026-84818	Unauthenticated Cross Site Scripting (XSS) in Open User Map <= 1.4.50 versions.	7.1	More Details
CVE-2026-84817	Unauthenticated Cross Site Scripting (XSS) in JetFormBuilder <= 3.6.5.1 versions.	7.1	More Details
CVE-2026-81798	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Easy Appointments allows DOM-Based XSS. This issue affects Easy Appointments: from n/a through 4.0.2.1.	7.1	More Details
CVE-2026-86091	ntopng before 6.7.260717 fails to check user privileges in the pools bulk-delete endpoint, allowing authenticated non-administrators to delete all host pools and member bindings. Attackers can issue POST requests to the delete pools endpoint to irreversibly destroy every host pool, removing traffic policy bindings and visibility restrictions that may bypass security policies.	7.1	More Details
CVE-2026-81781	Missing Authorization vulnerability in Unbounce Unbounce Landing Pages unbounce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Unbounce Landing Pages: from n/a through 1.1.4.	7.1	More Details
CVE-2026-19051	Plaintext storage of a password vulnerability in Menulux Software Inc. Menulux Portal allows Retrieve Embedded Sensitive Data. This issue affects Menulux Portal: before 20260903211448.	7.1	More Details
CVE-	Checkmate through 3.11.0 omits the isAllowed role guard middleware on maintenance-window, notification,		

2026-85390	and check-deletion routes, allowing read-only users to perform administrative actions. Attackers with user-role sessions can create arbitrary maintenance windows to silence alerts, modify notification channels, and delete monitor check history to erase incident evidence.	7.1	More Details
CVE-2026-82883	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marcus Login With Ajax allows Reflected XSS. This issue affects Login With Ajax: from n/a through 4.5.1.	7.1	More Details
CVE-2026-80113	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain a privilege escalation vulnerability in DirectIo64.sys that allows local users to clear arbitrary bits at any physical memory address due to missing validation of the physical address parameter in an exposed IOCTL handler. Attackers can obtain a device handle and supply an arbitrary 64-bit physical address with a bit index to invoke MmMapIoSpace and clear bits in kernel code pages or page table entries, enabling local privilege escalation or system compromise.	7.1	More Details
CVE-2026-80118	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain an unauthenticated physical memory disclosure in DirectIo64.sys, reachable by unprivileged local users through a single IOCTL with no caller-identity check. The handler writes a crash-dump-format (PAGEDU64) image of all physical memory to a caller-supplied file path in the SYSTEM context, allowing a standard user to create files in locations they cannot otherwise write and to recover memory belonging to processes of other users. The image is preceded by a header that exposes the kernel loaded-module list, active-process list and PFN database pointers, defeating KASLR. The same handler also dereferences the return value of an internal kernel-structure locator without a NULL check; that locator returns NULL on three distinct failure paths, and a kernel crash results on builds where any of those paths is taken.	7.1	More Details
CVE-2026-80130	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Relative Path Traversal vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to remote execution.	7.1	More Details
CVE-2026-86090	ntopng before 6.7.260717 fails to perform authorization checks in the delete endpoints and recipients REST v2 handlers. Authenticated non-administrator users can issue POST requests to irreversibly delete all configured notification endpoints and recipients, silencing all alerts.	7.1	More Details
CVE-2026-85395	UnoPim before 2.1.3 fails to include integration store, update, and key-generation routes in its ACL map, allowing any admin user to bypass permission checks. Attackers with minimal admin privileges can create OAuth API integrations, mint client credentials, and escalate permissions by exploiting missing authorization validation in the Bouncer middleware.	7.1	More Details
CVE-2026-80117	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain a privilege escalation vulnerability in DirectIo64.sys that allows local users to issue arbitrary IN and OUT instructions to any x86 I/O port due to missing allowlist or port validation on exposed IOCTLs. Attackers can obtain a device handle and write to sensitive ports including the PS/2 controller port, CPU reset ports, CMOS configuration ports, and interrupt controller ports to cause an immediate system reset or other hardware-level manipulation from a standard user account.	7.1	More Details
CVE-2026-84756	Subscriber Privilege Escalation in WCFM Membership <= 2.11.11 versions.	7.1	More Details
CVE-2026-80741	In the Linux kernel, the following vulnerability has been resolved: drm/log: Fix out-of-bounds read on empty message length drm_log_draw_kmsg_record() accesses s[len - 1] to strip the trailing newline, but len is unsigned int. If len is 0, the subtraction wraps to UINT_MAX, causing an out-of-bounds read. Add an early return when len is 0.	7.1	More Details
CVE-2026-84989	ntopng is a web-based network traffic monitoring application. In versions 6.7.0 through 6.7.260717, two REST v2 endpoints that manage ntopng's tag/badge feature — `POST /lua/rest/v2/delete/tag/tag.lua` and `POST /lua/rest/v2/edit/tag/tag.lua` — perform no authorization check at all. Any authenticated user, including a non-administrator ("unprivileged") account, can delete or rename any tag in the system, including tags created by an administrator. Version 6.7.260718 contains a fix.	7.1	More Details
CVE-2026-81295	Unauthenticated Cross Site Scripting (XSS) in Under Construction <= 5.82 versions.	7.1	More Details
CVE-2026-83961	ColdFusion is affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could leverage this vulnerability to gain limited read and write access. The vulnerable component is restricted to an administrative network zone by default. Exploitation of this issue does not require user interaction. Scope is changed.	7.1	More Details
CVE-2026-81292	Unauthenticated Cross Site Scripting (XSS) in Simple Payment <= 2.5.1 versions.	7.1	More Details

CVE-2026-86725	AVideo through c3edcc274c389816d434acadac07ee78eaf330c1 contains a missing authorization vulnerability in the SocialMediaPublisher plugin's add.json.php endpoint that allows authenticated users to modify other users' OAuth token records. Attackers can supply arbitrary row IDs to overwrite another user's stored access_token and refresh_token, then delete the compromised record to destroy the victim's provider linkage.	7.1	More Details
CVE-2026-81773	Unauthenticated Cross Site Scripting (XSS) in Ninja Forms File Uploads Extension <= 3.3.26 versions.	7.1	More Details
CVE-2026-84812	Unauthenticated Cross Site Scripting (XSS) in BP Better Messages <= 2.15.27 versions.	7.1	More Details
CVE-2026-84836	Subscriber Insecure Direct Object References (IDOR) in WC Ukraine Shipping <= 1.22.3 versions.	7.1	More Details
CVE-2026-81776	Unauthenticated Cross Site Scripting (XSS) in WP QuickLaTeX <= 3.8.8 versions.	7.1	More Details
CVE-2026-84848	Unauthenticated Cross Site Scripting (XSS) in Quick Event Manager <= 9.17 versions.	7.1	More Details
CVE-2026-85164	WWBN AVideo through commit c91b5975d contains a server-side request forgery vulnerability in the set_api_userImages API endpoint that fails to validate profileImg and backgroundImg URLs before fetching them. Authenticated API clients can supply internal URLs to fetch cloud metadata or internal services, with responses written to publicly accessible web paths for retrieval.	7.1	More Details
CVE-2026-20293	A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of Cisco UCS Servers and UCS-based appliances could allow an authenticated attacker with valid credentials for a user account with the role of user or admin or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software. This vulnerability is due to the availability of memory write commands in the UEFI Shell while UEFI Secure Boot is enabled on a device. An attacker could exploit this vulnerability by selecting the UEFI Shell boot option at boot time and using available shell commands to modify UEFI memory variables. A successful exploit could allow the attacker to manipulate the preboot environment, overwrite UEFI Secure Boot-related memory values, and execute unauthorized software on the affected device.	7.1	More Details
CVE-2026-81300	Unauthenticated Cross Site Scripting (XSS) in Calculation For Contact Form 7 <= 1.0 versions.	7.1	More Details
CVE-2026-84763	Unauthenticated Cross Site Scripting (XSS) in RTMKit <= 2.1.5 versions.	7.1	More Details
CVE-2026-84765	Unauthenticated Cross Site Scripting (XSS) in Breadcrumb NavXT <= 7.5.1 versions.	7.1	More Details
CVE-2026-80749	In the Linux kernel, the following vulnerability has been resolved: drm/connector/hdmi: Fix out of bounds memory read A helper function was copying a given audio infoframe into the connector's copy but using the size of the destination (a generic target, sized to accept many different data blocks) not the source (a very specific type of data block). Thus, it was copying 60 bytes of data from a 28 byte allocation. Fix that by using the source size instead, together with a build bug on the source size actually being smaller than the destination. I hit this running KUnit tests under KASAN (while debugging something else entirely). In the real world, it seems unlikely to cause an actual problem. It is a read not a write so it can't corrupt any memory. However, it could potentially fall off the end of a page and cause an accvio bug.	7.1	More Details
CVE-2026-71220	A stack out-of-bounds write vulnerability was found in gfs2-utils. In gfs2_edit, the di_height field from on-disk inode metadata is used as an array index without bounds checking, causing a stack buffer overflow that may lead to arbitrary code execution when processing crafted GFS2 filesystem images.	7.0	More Details
CVE-2026-71221	A stack out-of-bounds write vulnerability was found in gfs2-utils. In savemeta, the height value from on-disk inode metadata is used as a loop bound without bounds checking, causing a stack buffer overflow that may lead to arbitrary code execution when processing crafted GFS2 filesystem images.	7.0	More Details
CVE-	The X-mount.subdir option uses a detached-tree fast path on Linux 6.15 and later and passes the configured subdirectory to open_tree() with AT_SYMLINK_NOFOLLOW. That flag does not stop intermediate symlink		More

2026-78409	traversal or keep resolution inside the newly mounted filesystem. A local unprivileged user with an fstab-authorized X-mount.subdir entry can attach a host path at the intended mountpoint.	7.0	Details
CVE-2026-86143	In xmlIO in libxml2 before 2.15.4, an inconsistency in xmlOutputWriteCallback and xmlBufUse causes negative lengths to reach write callbacks, aka a lack of a check for integer overflow before calling writecallback. This has security relevance for many types of uses of that length value within a callback.	6.9	More Details
CVE-2026-86139	In libxml2 before 2.15.4, xmlURIEscapeStr in uri.c has an integer overflow.	6.9	More Details
CVE-2026-86138	In libxml2 before 2.15.4, xmlDictAddQString in dict.c has an integer overflow and resultant heap-based buffer overflow.	6.9	More Details
CVE-2026-86142	In libxml2 before 2.15.4, there is a heap-based buffer overflow in xmlXPtrEvalXPtrPart because of xmlXPtrEval xpointer length saturation.	6.9	More Details
CVE-2026-55421	Open edX Platform enables the authoring and delivery of online learning at any scale. Prior to commit 00b7c3c, the endpoint accepts user-supplied files[].url, performs a server-side fetch using "requests.get(url, allow_redirects=True)". The fetched bytes are then returned inside a ZIP response. This enables SSRF with response exfiltration. Redirect-following is enabled, and there is no timeout in the vulnerable fetch path. This issue has been patched via commit 00b7c3c.	6.8	More Details
CVE-2026-84028	The Bold Page Builder WordPress plugin before 5.9.9 does not sanitise and escape a shortcode attribute before outputting it in an HTML attribute, allowing users with the Contributor role and above to inject arbitrary web scripts that execute when a user views the affected page.	6.8	More Details
CVE-2026-86497	In JetBrains YouTrack before 2026.2.18769 changing a mailbox host without re-authentication allowed a project administrator to exfiltrate stored mailbox credentials	6.8	More Details
CVE-2026-68860	Dell PowerProtect Data Manager, versions 20.2.0.0 and below, contain a Reliance on Data/Memory Layout vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to Launch of phishing attacks.	6.8	More Details
CVE-2025-15664	The Ultimate Before After Image Slider & Gallery WordPress plugin before 4.7.19 does not properly escape the slider's before-label value before its bundled client-side script re-injects it into the DOM, allowing users with the Author role and above to store a payload that executes in the browser of anyone (including an administrator) who views the slider.	6.8	More Details
CVE-2025-15663	The Ultimate Before After Image Slider & Gallery WordPress plugin before 4.7.19 does not properly escape the slider's after-label value before its bundled client-side script re-injects it into the DOM, allowing users with the Author role and above to store a payload that executes in the browser of anyone (including an administrator) who views the slider.	6.8	More Details
CVE-2026-73313	XenForo before 2.3.13 contains a multi-factor authentication bypass vulnerability in the passkey TFA provider that allows an authenticated attacker to complete login as another user by submitting their own registered passkey credential during the WebAuthn assertion step. The passkey verification path performs a global credential lookup without validating that the matched credential belongs to the user whose login is pending, enabling an attacker who knows a target account's password to sign the challenge with their own passkey and bypass multi-factor authentication on both public forum and ACP login paths.	6.8	More Details
CVE-2026-74859	The shell theme installer in gnome-tweaks extracts user-supplied ZIP archives without validating archive member paths. As a result, a crafted theme archive can write files outside ~/.themes by using ../ path traversal, absolute paths, or symlink entries.	6.8	More Details
CVE-2026-74853	The Pods WordPress plugin before 3.3.9.2 does not restrict which functions a display callback may resolve to, allowing users with the author role and above to read arbitrary files from the server, including files outside the web root. Only sites using the restricted display-callback mode are affected, which is the automatic default on installations whose first Pods version predates 3.1.	6.8	More Details
CVE-2026-62654	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). A special maintenance mode can be activated via a physical key sequence during device boot, in which the device downloads and executes program code from a network server without verifying its authenticity or integrity. This could allow an attacker with physical access to the device to upload and execute arbitrary, unsigned code.	6.8	More Details
CVE-2026-83544	The Greenshift WordPress plugin before 13.2.0 does not properly escape a block animation attribute before outputting it within an HTML attribute, allowing users with contributor-level access and above to inject arbitrary web scripts that execute when the content is viewed.	6.8	More Details

CVE-2026-84931	The Joli Table Of Contents WordPress plugin before 3.0.3 does not sanitise or escape a shortcode attribute value before outputting it inside an HTML element's attribute, allowing users with the Author role and above to inject arbitrary HTML attributes and JavaScript that execute in the browser of any user who views the post, including higher-privileged users such as administrators. This crosses a privilege boundary even on multisite, where such users are not permitted to post unfiltered HTML.	6.8	More Details
CVE-2026-84930	The CatFolders Document Gallery & PDF Library WordPress plugin before 2.0.7 does not properly validate a block attribute before using it as an HTML tag name in its gallery output, allowing users with the Author role and above to inject arbitrary web scripts that execute in the browser of anyone who views the affected post.	6.8	More Details
CVE-2026-84937	The Video Player for YouTube WordPress plugin before 2.1.0 does not properly sanitise and escape user-supplied input before using it in a SQL statement, allowing users with the Contributor role and above to perform SQL injection attacks and read arbitrary data from the database.	6.8	More Details
CVE-2026-84899	The VikWidgetsLoader WordPress plugin before 1.12.0 does not sanitise or escape a block attribute before outputting it inside an inline script, allowing users with the Contributor role to store arbitrary JavaScript that executes in the browser of any user viewing the affected post, including the administrator who reviews the pending submission.	6.8	More Details
CVE-2026-86254	wger versions through master contain an incomplete authorization bypass in wger/core/views/user.py where three views retain the original gym-scope check using raw integer comparison instead of the is_same_gym() helper, allowing gym staff with gym=None to delete, deactivate, or activate any other user with gym=None. Attackers with gym.manage_gym permission and gym=None affiliation can permanently delete user accounts, lock users out via deactivation, or undo defensive deactivations by exploiting the None != None comparison edge case.	6.8	More Details
CVE-2026-12704	When SAML IdP-initiated login is enabled in Grafana Enterprise, the SAML library skips validation of the InResponseTo field on all SAML responses, including SP-initiated logins. This removes anti-replay protection, allowing an attacker who obtains a valid signed SAML assertion to replay it and gain a session as the victim user. Only instances with the allow_idp_initiated SAML setting enabled are affected; this setting is off by default and Grafana OSS is not affected.	6.8	More Details
CVE-2026-84221	The Kirki WordPress plugin before 6.3.0 does not escape a user-supplied identifier before using it in a SQL query, allowing users with editor-level access and above to append arbitrary SQL and read the contents of the database, including user credentials.	6.8	More Details
CVE-2026-84022	The Bold Page Builder WordPress plugin before 5.9.8 does not sanitise and escape several shortcode attributes before outputting them in HTML attributes, allowing users with the Contributor role and above to inject arbitrary web scripts that execute when a user views the affected page.	6.8	More Details
CVE-2026-84021	The Bold Page Builder WordPress plugin before 5.9.8 does not properly validate a link URL before outputting it in an HTML attribute, relying on a filter that can be evaded, allowing users with the Contributor role and above to inject arbitrary web scripts that execute when a user clicks the affected link.	6.8	More Details
CVE-2026-83547	The Xpro Addons WordPress plugin before 1.7.4 does not properly escape some of its widgets' settings before outputting them within HTML attributes, which could allow users with the Contributor role and above to perform Stored Cross-Site Scripting attacks.	6.8	More Details
CVE-2026-84896	The King Addons for Elementor WordPress plugin before 51.1.77 does not escape a widget display-style setting before outputting it in an HTML attribute, allowing users with Contributor-level access and above to store JavaScript that executes in the browser of any visitor to the affected page, including logged-in administrators.	6.8	More Details
CVE-2026-19719	The Social Media Share Buttons & Social Sharing Icons WordPress plugin before 3.0.1 does not escape the post title before outputting it in an inline JavaScript event handler, allowing users with the Contributor role and above to perform Stored Cross-Site Scripting attacks which are triggered when a visitor interacts with the affected button. Exploitation requires the Social Media Share Buttons & Social Sharing Icons WordPress plugin before 3.0.1 to be running a non-default icon display configuration.	6.8	More Details
CVE-2026-82846	The Masteriyo LMS WordPress plugin before 3.4.0 does not sanitise and escape some course settings before outputting them in a page available to all visitors, allowing users with a course-author role to perform Stored Cross-Site Scripting attacks that run in the session of anyone viewing the course, including a logged-in administrator.	6.8	More Details
CVE-2026-62653	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). The input received over a proprietary communication protocol that is exposed when the device is placed into a special firmware-update mode is not properly validated, resulting in a memory corruption condition. This could allow an unauthenticated attacker with physical access to the device to cause a crash and potentially execute arbitrary code on the device.	6.8	More Details
CVE-2026-	SolidInvoice is an open-source invoicing platform. Prior to version 3.0.1, `UserInvitation` entities have no expiry timestamp. Invitation links mailed to users remain valid indefinitely, meaning a leaked, forwarded, or archived invitation email can be used at any time in the future to join a company or silently add a	6.8	More Details

61608	compromised email account to a company. Version 3.0.1 fixes the issue.		
CVE-2026-82884	The All in One SEO WordPress plugin before 5.0.0.1 does not sanitise and escape some content stored in posts before rendering it back in the post editor, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks that trigger when a higher privileged user edits the post.	6.8	More Details
CVE-2026-20510	In camera middleware, there is a possible escalation of privilege due to double free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11134622; Issue ID: MSV-8894.	6.7	More Details
CVE-2021-43614	Error in handling the PlatformLangCodes UEFI variable could cause a buffer overflow, leading to resource exhaustion and failure.	6.7	More Details
CVE-2026-20512	In Audio HAL, there is a possible escalation of privilege due to improper input validation. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11087540; Issue ID: MSV-8246.	6.7	More Details
CVE-2026-20511	In SurfaceFlinger, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11123860; Issue ID: MSV-8890.	6.7	More Details
CVE-2026-20506	In Audio HAL, there is a possible escalation of privilege due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11191981; Issue ID: MSV-9126.	6.7	More Details
CVE-2026-20508	In Power HAL, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11165543; Issue ID: MSV-9012.	6.7	More Details
CVE-2026-20507	In Audio HAL, there is a possible escalation of privilege due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11191981; Issue ID: MSV-9125.	6.7	More Details
CVE-2026-20517	In geniezone, there is a possible escalation of privilege due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10900510; Issue ID: MSV-6781.	6.7	More Details
CVE-2026-5522	IBM QRadar 7.5.0 through 7.5.0 UP15 Interim Fix 005 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	6.7	More Details
CVE-2026-20509	In Power HAL, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11165543; Issue ID: MSV-9011.	6.7	More Details
CVE-2026-10821	The Yoast SEO Premium WordPress plugin before 27.6.1 does not sanitize control characters from redirect origins before writing them to the site's Apache configuration file when the file-based redirect mode is enabled, and the redirect-creation endpoint is reachable by users with only Author-level access. This allows such users to inject arbitrary newline-delimited Apache directives into the root .htaccess file. On Apache servers that honour PHP directives, the injection can be chained with the user's own media upload (a polyglot image carrying a PHP payload) and an auto_prepend_file directive to achieve Remote Code Execution.	6.6	More Details
CVE-2026-84898	The Eventin WordPress plugin before 4.1.21 does not properly validate a template path value before using it to include a local file, allowing users with contributor-level access and above to include and execute arbitrary local PHP files.	6.6	More Details
CVE-2026-85092	LiME through 1.12.0 fails to validate the disk acquisition output path and does not use O_NOFOLLOW when opening the operator-supplied path parameter, allowing unprivileged local users to overwrite arbitrary root-owned files. An attacker who controls the output directory can create a symbolic link with the expected filename pointing to any root-owned file, and when the acquisition runs in kernel context, LiME follows the link and truncates the target file with the memory acquisition stream.	6.6	More Details
CVE-2026-84769	Unauthenticated Insecure Direct Object References (IDOR) in Business Directory <= 6.4.26 versions.	6.5	More Details
CVE-2026-86734	Snipe-IT before 8.7.1 fails to validate the length of the note field in the POST /account/accept/{acceptance} endpoint, allowing authenticated users to submit unbounded input that reaches synchronous CommonMark rendering. Attackers can submit large note values to exhaust PHP worker CPU and cause denial of service through resource exhaustion in the markdown parsing pipeline.	6.5	More Details

CVE-2026-82223	Unauthenticated Broken Access Control in WP Event SOlution <= 4.1.22 versions.	6.5	More Details
CVE-2026-85089	FreeRDP versions 3.0.0 through 3.30.0 (before 3.31.0) transmit uninitialized heap memory in Save Session Info PDU reserved padding fields. Three PDU writers in libfreerdp/core/info.c (rdp_write_logon_info_v2, rdp_write_logon_info_plain, and rdp_write_logon_info_ex) use Stream_Seek instead of Stream_Zero for reserved pad bytes (up to 576 bytes), leaving previously freed heap contents in the outgoing PDU. Because the send buffer is allocated with malloc (not zeroed), stale heap data — which may include cleartext credentials from prior sessions — can be sent to the receiving peer. FreeRDP-based servers using rdpUpdate::SaveSessionInfo and freerdp-proxy (which forwards these PDUs) are affected, allowing disclosure of server/proxy process memory to a downstream client.	6.5	More Details
CVE-2026-27086	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xtemos WoodMart allows DOM-Based XSS. This issue affects WoodMart: from n/a before 8.3.8.	6.5	More Details
CVE-2026-81666	An integer overflow was found in Corosync's handling of membership commit token messages. The length-validation check for these messages can be bypassed on 32-bit systems due to an integer overflow in the calculation of the expected message length, allowing a crafted network packet to trigger an out-of-bounds memory access that crashes the Corosync daemon. This results in a denial of service for the affected cluster node. The overflow does not occur on 64-bit systems, where the length calculation is correctly performed in 64-bit arithmetic.	6.5	More Details
CVE-2026-74769	Dell PowerProtect Data Manager, versions 20.2.0.0 and below, contain an Incorrect Authorization vulnerability in the REST API. A low privileged remote attacker could potentially exploit this vulnerability, leading to Protection mechanism bypass.	6.5	More Details
CVE-2026-85163	AVideo through commit c91b5975d contains a server-side request forgery vulnerability in the EPG parser that allows authenticated uploaders to fetch arbitrary internal URLs. An attacker can supply an internal URL via the epg_link parameter during video upload, which is validated only for syntax and later fetched server-side during EPG generation without SSRF protection checks.	6.5	More Details
CVE-2026-86597	Insertion of sensitive information into log files in the Snowflake Python, Go, JDBC, Node.js, PHP PDO, and ODBC drivers allowed authentication tokens, query-result encryption keys, pre-signed cloud-storage URLs, and SAML assertions to be written to diagnostic logs in circumstances where the available log redaction did not cover all affected log paths and data types. An attacker with read access to the log destination, whether the local filesystem, a log aggregation service, or a CI/CD artifact store, could obtain credentials and decryption keys that, if still valid at the time of access, could be used to authenticate to the corresponding Snowflake account or cloud-storage object. Successful exploitation requires read access to the log destination, and impact is bounded by credential lifetime and object scope. The fix is available in the patched versions listed above. Users must manually upgrade and should securely delete previously generated diagnostic logs containing sensitive information where retention is not required.	6.5	More Details
CVE-2026-86731	Craft CMS versions 5.0.0-RC1 through 5.10.11 are missing an admin-target guard in UsersController::actionActivateUser (the users/activate-user action). While the action requires the administrateUsers permission, it does not call requireAdmin() when the targeted user is an administrator, unlike the mirror action actionDeactivateUser. As a result, an authenticated control panel user who is not an administrator but holds the administrateUsers permission can activate a pending or deliberately deactivated administrator account, which can lead to permission escalation when combined with resetting that account's password. The issue is fixed in Craft CMS 5.10.12.	6.5	More Details
CVE-2026-81792	Unauthenticated Privilege Escalation in Product Catalog Enquiry for WooCommerce by MultiVendorX <= 6.1.4 versions.	6.5	More Details
CVE-2026-14215	The Booking for Appointments and Events Calendar WordPress plugin before 2.4.9 does not require authentication or a valid request token before running the post-booking action chain, allowing an unauthenticated user to trigger booking notifications and integration callbacks for a booking by enumerating its identifier.	6.5	More Details
CVE-2026-18021	The The Beaver Builder Page Builder – Drag and Drop Website Builder plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.10.3.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	6.5	More Details
CVE-2026-86550	NuBrowser lacks protocol whitelist validation for the S.browser_fallback_url field of intent://, allowing attackers to inject javascript: URLs via 302 redirects. This results in a universal cross-site scripting (UXSS) vulnerability that enables script execution within the origin of arbitrary websites.	6.5	More Details
CVE-2026-	Unauthenticated Insecure Direct Object References (IDOR) in WpEvently <= 5.6.0 versions.	6.5	More

81802			Details
CVE-2026-17509	The WPML Multilingual CMS plugin for WordPress is vulnerable to time-based SQL Injection via the 'elementIds' parameter in all versions up to, and including, 4.9.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This vulnerability is exploitable due to an authorization bypass where the registered authorization callback fails to execute, allowing any authenticated user regardless of role to access administrative translation functionalities.	6.5	More Details
CVE-2026-82076	An integer overflow in the query planning component of MongoDB Server can allow an authenticated user with ordinary database-level read/write privileges to bypass an internal resource limit. Submitting a specially crafted query causes the server to consume memory without bound during query planning, and the resulting exhaustion terminates the server process. This may result in a denial of service affecting all databases served by the affected node.	6.5	More Details
CVE-2026-85162	AVideo through commit c91b5975d contains a cross-site request forgery vulnerability in plugin/Live/saveLive.php that lacks forbidIfNotPost and forbidIfInvalidToken protections. Attackers can craft malicious image tags to overwrite authenticated streamers' RTMP keys, passwords, and titles, hijacking live broadcasts.	6.5	More Details
CVE-2026-83562	Contributor Cross Site Scripting (XSS) in WCFM Marketplace <= 3.8.2 versions.	6.5	More Details
CVE-2026-84758	Unauthenticated Broken Access Control in Business Directory <= 6.4.26 versions.	6.5	More Details
CVE-2026-85578	SiYuan through 3.8.1 contains an authorization bypass vulnerability in the /api/file/getFile endpoint that allows readers to retrieve files from notebooks explicitly configured as Visible:false. Attackers with reader role can access private workspace files including notebook metadata and internal configuration by knowing the hidden notebook identifier and file path.	6.5	More Details
CVE-2026-85693	Chatbot UI contains an authorization bypass vulnerability in the retrieval endpoint that allows authenticated attackers to access private file content belonging to other users by supplying arbitrary file UUIDs. The endpoint uses a service-role Supabase client that bypasses row-level security and fails to validate file ownership, enabling attackers to retrieve indexed content chunks from victim files through crafted POST requests.	6.5	More Details
CVE-2026-78599	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) in the Kibana Fleet feature can lead to the unauthorized deletion of internal resources via Path Traversal (CAPEC-126). A low-privileged user holding Fleet write access could cause a subsequent administrative delete action to act on unintended internal resources. Exploitation requires an administrator to interact with the affected Fleet interface.	6.5	More Details
CVE-2026-18887	IBM i 7.6, 7.5, 7.4, and 7.3 could allow an authenticated attacker to obtain sensitive information in PASE. An attacker could exploit this vulnerability to access information about process they shouldn't be permitted to access.	6.5	More Details
CVE-2026-9186	IBM Langflow OSS 1.0.0 through 1.11.2 allows remote authenticated attackers to bypass localhost-only MCP configuration installation by spoofing X-Forwarded-For: 127.0.0.1 header, enabling arbitrary writes to IDE config files (~/.cursor/mcp.json, etc.).	6.5	More Details
CVE-2026-9138	IBM Langflow OSS 1.0.0 through 1.11.2 Langflow could allow an authenticated attacker to write arbitrary files to the server due to improper input validation in the SaveToFileComponent. The application constructs local file paths using attacker-controlled input without sufficient sanitization when handling requests to the /api/v1/run/{flow_id} endpoint. An attacker with low-privileged authenticated access (such as a valid API key or user session) can supply crafted path values, including absolute paths or path traversal sequences, allowing arbitrary file writes to locations writable by the Langflow process. Successful exploitation may lead to unauthorized file creation or modification, potentially resulting in further compromise depending on the deployment environment.	6.5	More Details
CVE-2026-74236	GFI Exinda AI and ClearView before 7.6.5 contains a path traversal vulnerability in the diagnostic file deletion handler. The unlink_or_email_file() function accepts parameters prefixed with v_file_row_ and appends their values directly to a base directory path without sanitizing for directory traversal sequences. An authenticated attacker with Admin privileges can delete arbitrary files from the system in the context of root.	6.5	More Details
CVE-2026-	GFI Exinda AI and ClearView before 7.6.5 contains an argument injection vulnerability in the Tools Iperf Client functionality. The web_tools_cmd() function constructs an iperf command using the server and options parameters without sanitization, permitting injection of arbitrary iperf flags. An authenticated attacker with	6.5	More Details

74237	Unprivileged (lowest-level) access can supply the iperf -F flag to read an arbitrary file from the system and transmit its contents to an attacker-controlled server.		
CVE-2026-85700	Onyx 4.6.6 fails to properly restrict access to custom tool credentials stored in custom_headers, allowing any authenticated user to read admin-defined API keys. Attackers with basic authentication can call GET /tool/{tool_id} or GET /tool endpoints to retrieve plaintext authorization headers and third-party API credentials, then use them to directly access upstream APIs.	6.5	More Details
CVE-2026-85697	Documenso 2.17.0 contains an access control vulnerability in the PDF-serving endpoint that fails to validate document visibility settings. Attackers with low privileges can read restricted documents within their team or cross-tenant by leveraging missing ownership validation on document data identifiers.	6.5	More Details
CVE-2026-85692	Nightingale (n9e), as of commit 8362cbe (main branch, confirmed 2026-08-27), contains a server-side request forgery vulnerability in the isPublicIP function in aiagent/tools/http.go, the SSRF guard for the http_fetch AI-agent tool. The function only unwraps standard IPv4-mapped (::ffff:a.b.c.d) IPv6 addresses before checking them against the forbidden-range list, and does not classify 6to4 (2002::/16), NAT64 (64:ff9b::/96, 64:ff9b:1::/48), or deprecated site-local (fec0::/10) addresses. On a dual-stack or NAT64-enabled host, an attacker able to supply a URL to the http_fetch tool can bypass the guard by encoding a forbidden IPv4 address (such as the cloud instance-metadata endpoint 169.254.169.254) in one of these IPv6 forms to reach internal or metadata services.	6.5	More Details
CVE-2026-75602	OpenList a file list program that supports multiple storage. Prior to 4.2.3, OpenList's offline-download feature at POST /api/fs/add_offline_download with tool: "SimpleHttp" accepts an attacker-supplied URL and saves its bytes under a per-task temporary directory before transferring them to the user's destination storage. The temporary filename comes from the attacker-controlled Content-Disposition header, is passed from parseFilenameFromContentDisposition in internal/offline_download/http/util.go to filepath.Join(task.TempDir, filename) in SimpleHttp.Run in internal/offline_download/http/client.go, and is opened with os.Create without a containment check. Because filepath.Join cleans .. segments, a non-admin user with PermAddOfflineDownload on any path can traverse out of task.TempDir and create, truncate, or overwrite any file writable by the OpenList process whose parent directory already exists. The server/handles/offline_download.go AddOfflineDownload route uses normal user authentication rather than AuthAdmin, and local-storage destinations fall through tryPutUrl in internal/offline_download/tool/add.go to the vulnerable SimpleHttp.Run path. This issue is fixed in version 4.2.3.	6.5	More Details
CVE-2026-85689	llmware 0.4.6 contains an SQL injection vulnerability in the collection-database layer (llmware/resources.py) where filter and lookup values are directly string-interpolated into SQL WHERE clauses without parameterization or escaping, in both the SQLite and PostgreSQL backends. The filter validator only checks keys against an allow-list and never sanitizes values. Attacker-controlled filter values reaching the public API via Library.block_lookup and Query.text_query_with_custom_filter / text_query_by_author_or_speaker can neutralize the intended filter to disclose rows the caller was scoped out of (cross-document/cross-collection disclosure); on PostgreSQL the flaw permits boolean- and UNION-based SQL injection.	6.5	More Details
CVE-2026-85670	tokenizers (Hugging Face) is affected by an out-of-bounds buffer access in BpeBuilder::build (tokenizers/src/models/bpe/model.rs). When loading a tokenizer.json via Tokenizer::from_file/from_str, the builder sizes a scratch buffer to the longest vocabulary key, then writes each concatenated merge rule into it. A merge whose concatenated token exceeds the longest vocabulary key overruns the buffer, which Rust turns into a panic that aborts the process in Rust and FFI embeddings. This occurs at load time with no encoding required, so an attacker who supplies a crafted tokenizer.json can cause a denial of service. A secondary defect at the same location can cause a usize underflow (panic in debug, potential memory corruption in release) when continuing_subword_prefix is set and a merge token is shorter than the prefix. Observed in version 0.23.1.	6.5	More Details
CVE-2026-85669	potpie through 2.0.0 fails to verify user ownership on the POST /conversations/{conversation_id}/code-changes/sync endpoint. Authenticated attackers can write arbitrary file changes into other users' conversations by supplying their conversation IDs, allowing unauthorized modification of pending changes.	6.5	More Details
CVE-2026-85665	Bruno versions through 4.1.0 fail to validate file paths in request body declarations, allowing attackers to read arbitrary local files by using parent-directory traversal segments. When a collection is executed, attackers can craft a request with a body:file path containing ../ sequences that resolve outside the collection directory, causing the application to read and exfiltrate arbitrary files to attacker-controlled endpoints.	6.5	More Details
CVE-2026-19475	An authenticated user with permission to query a SQL data source can bypass the fix for CVE-2026-33375 by injecting the timeGroup macro through a WHERE clause, which Grafana's regex-based macro parsing does not reject. Evaluating the injected macro causes uncontrolled memory consumption that can terminate the Grafana server process, resulting in a denial of service. The Microsoft SQL Server, PostgreSQL, and MySQL data sources are affected.	6.5	More Details
CVE-2026-85624	Blinko 1.8.7 contains a cross-user private note disclosure vulnerability in the noteReferenceList procedure that performs no ownership verification on supplied note identifiers. Authenticated attackers can enumerate sequential note IDs and retrieve complete content of other users' private notes including attachments and tags.	6.5	More Details

CVE-2026-84215	Unauthenticated Broken Access Control in Timetics <= 1.0.61 versions.	6.5	More Details
CVE-2026-85621	LobeChat (LobeHub) 2.2.1 does not properly verify inbound chat-platform webhook signatures in the QQ and Feishu adapters. The webhook route (/api/agent/webhooks/:platform) is unauthenticated by design and delegates verification to each adapter; the QQ adapter performs no Ed25519 signature verification on dispatched message events, and the Feishu adapter only performs an optional static-token comparison that is skipped when no token is configured (the default) and is not a body signature. An unauthenticated attacker who knows the public webhook URL can POST forged inbound messages with an attacker-chosen sender identity and arbitrary text, causing the bot owner's agent to process attacker-controlled input and treat the attacker as a trusted platform sender.	6.5	More Details
CVE-2026-19299	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote authenticated attacker to obtain sensitive information due to path traversal.	6.5	More Details
CVE-2026-19302	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of symbolic links.	6.5	More Details
CVE-2026-84754	Unauthenticated Broken Access Control in WPFunnels <= 3.12.13 versions.	6.5	More Details
CVE-2026-78588	Allocation of Resources Without Limits or Throttling (CWE-770) in Filebeat can lead to a denial of service via Excessive Allocation (CAPEC-130). An attacker able to reach the Filebeat HTTP ingestion endpoint could send specially crafted compressed requests that exhaust the memory resources of the Filebeat process.	6.5	More Details
CVE-2026-85580	SiYuan versions before v3.8.2 contain a path guard bypass vulnerability in the MCP file-access handler that uses case-sensitive matching on Linux filesystems. Attackers can read the protected publishAccess.json file by requesting case-variant paths like PublishAccess.json to disclose sensitive publish-access configuration and metadata.	6.5	More Details
CVE-2026-85582	SiYuan versions before v3.8.2 contain an unbounded session creation vulnerability in the publish-service Basic Auth handler that allows authenticated attackers to exhaust memory. Attackers can repeatedly authenticate with valid credentials to create persistent session entries without expiry or capacity limits, causing indefinite process memory growth and denial of service.	6.5	More Details
CVE-2026-85583	SiYuan versions before v3.8.2 contain a path traversal vulnerability in the reader-accessible file-read endpoint that follows symlinks when opening authorized asset paths. Attackers with reader role can request a logical asset under data/assets/ that is a symlink to a file outside the workspace and receive the target file bytes, bypassing workspace boundary restrictions.	6.5	More Details
CVE-2026-78970	JeecgBoot 3.9.2 and earlier contains an authorization bypass vulnerability in the SystemApiController component. An authenticated attacker with any valid JWT token can access multiple API endpoints (including queryAllUser, queryUsersByUsernames, queryUserById, and queryUsersByIds) to retrieve sensitive information of all users, including real names, phone numbers, email addresses, employee numbers, and role definitions, due to missing fine-grained permission checks and incomplete data desensitization.	6.5	More Details
CVE-2026-78658	IBM UCD - IBM UrbanCode Deploy 7.2 through 7.2.3.25, and 7.3 through 7.3.2.20 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.15, 8.1 through 8.1.2.8, and 8.2 through 8.2.2.1 IBM DevOps Deploy / IBM UrbanCode Deploy (UCD) is susceptible to an formation disclosure vulnerability when processing redacted property values. If a deployment is configured with a secure property that starts with certain non-ASCII characters, the redaction engine may fail to mask subsequent ASCII secure values embedded inside unsecure properties. An authenticated user with permissions to view deployment request details could exploit this flaw via the UI or API to view sensitive values in plain text that should otherwise be redacted.	6.5	More Details
CVE-2026-85093	Cheshire Cat AI's GET /memory/collections/{collection_id}/points endpoint fails to apply per-user filtering when retrieving episodic memory points. Authenticated attackers with MEMORY:READ permission can retrieve all users' stored conversation messages and personal data by paginating through the collection using the offset cursor.	6.5	More Details
CVE-2026-81281	Subscriber Cross Site Scripting (XSS) in Graphene <= 2.9.4 versions.	6.5	More Details
CVE-2026-78586	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user with low-level privileges could submit a specially crafted request that causes Kibana to consume an unbounded amount of memory, rendering it unavailable to all users.	6.5	More Details
CVE-			

2026-81282	Subscriber Cross Site Scripting (XSS) in Product Variations Swatches for WooCommerce <= 1.1.18 versions.	6.5	More Details
CVE-2026-82074	MongoDB Server contains an incorrect authorization vulnerability in the aggregation framework. An authenticated user with minimal privileges can craft a specially formatted aggregation request that causes the server's authorization subsystem to evaluate a different operation than what is actually executed, resulting in unauthorized read access to collection data within the target database.	6.5	More Details
CVE-2026-75165	An issue in /cgi-bin/wwwugw.cgi of MBS-Solutions X-Serie Gateway firmware V6_00_05 allows a remote authenticated user with the low-privileged Standard role to invoke hidden network diagnostic methods (ugw-ping, ugw-traceroute) that are not exposed in the web UI, allowing attackers to obtain sensitive information.	6.5	More Details
CVE-2026-75164	An arbitrary file read vulnerability in /cgi-bin/ugwdownload.cgi of MBS-Solutions X-Serie Gateway firmware V6_00_05 allows a remote authenticated user with the low-privileged Standard role to retrieve arbitrary files from the device filesystem via the file query string parameter.	6.5	More Details
CVE-2026-73321	XenForo before 2.3.13 contains an uncontrolled recursion vulnerability in the BBCode parser that allows authenticated attackers to cause persistent denial of service by submitting a post with deeply nested BBCode tags. Attackers can craft a single malicious post with sufficient nesting depth to exceed PHP's stack limit, causing fatal errors that repeatedly terminate PHP-FPM workers for all visitors rendering the affected thread.	6.5	More Details
CVE-2026-75163	An information disclosure vulnerability in the ugw-deviceinfo method of /cgi-bin/wwwugw.cgi in MBS-Solutions X-Serie Gateway firmware V6_00_05 returns detailed system version fields (operatingsystem, gatewayversion) to any authenticated user, including users with the low-privileged Standard role.	6.5	More Details
CVE-2026-19645	IBM MQ Agent CD: v1.0.0, v1.0.1, v2.0.0, v2.0.1 An authenticated user with a valid session cookie can submit arbitrarily large or computationallyexpensive requests that cause the LLM agent workers to be held for extended periods — rangingfrom tens of seconds to over ten minutes per request. When multiple such requests are sentconcurrently, the agent worker pool becomes exhausted, causing all other IBM MQ Console users toexperience degraded performance or complete unavailability of the AI Agent feature.	6.5	More Details
CVE-2026-85603	Grav versions before 1.10.55 contain a path traversal vulnerability in the admin plugin's Save As action that fails to validate the language code parameter. An authenticated admin user with admin.pages.create permission can supply directory traversal sequences in the lang POST field to write arbitrary .md files outside the pages directory with attacker-controlled content.	6.5	More Details
CVE-2026-84755	Unauthenticated Broken Access Control in Mail Mint <= 1.31.0 versions.	6.5	More Details
CVE-2026-84809	Tencent AI-Infra-Guard's skill-scan component excludes compiled Python bytecode files from analysis by hardcoding __pycache__ directories and .pyc/.pyo/.pyd extensions into skip lists across multiple scanning surfaces. Attackers can distribute skills with benign Python source files alongside malicious compiled bytecode that executes on import while the scanner reports a safe verdict, enabling code execution when operators install the skill.	6.5	More Details
CVE-2022-51018	PocketMine-MP before 3.26.5 and 4.0.x before 4.0.5 does not limit book page text length, page count, or author/title length. A player who obtains a writable book can create oversized NBT ('book bombs'), causing excess bandwidth consumption and server crashes (exceeding the 1 MB chunk size limit when saving region-based worlds in PM3, or exceeding the 32 KiB TAG_String limit in PM4).	6.5	More Details
CVE-2026-55221	Boruta is a standalone authorization server that aims to implement OAuth 2.0 and Openid Connect up to decentralized identity specifications. Prior to version 0.10.0, Boruta logged sensitive OAuth and OpenID Connect values in business event logs. Logged values could include access tokens, refresh tokens, authorization codes, agent tokens, direct-post codes, ID tokens, VP tokens, and tokens submitted to introspection or revocation endpoints. An attacker with access to Boruta logs, log aggregation systems, or the administration log viewer could recover these credentials and use them until expiration or revocation. This issue has been patched in version 0.10.0.	6.5	More Details
CVE-2026-12757	The The Email Subscribers & Newsletters – Email Marketing, Post Notifications & Newsletter Plugin for WordPress plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.9.27. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	6.5	More Details
CVE-2026-86097	PX4 Autopilot through 1.17.0 contains a null pointer dereference vulnerability in param_set_default_file() and param_set_backup_file() functions that allows attackers to crash the autopilot process. Attackers can invoke 'param select' or 'param select-backup' commands with no path argument from any PX4 shell to trigger the crash.	6.5	More Details
CVE-2026-	Information leak in MediaCapture in Google Chrome prior to 152.0.7977.75 allowed a remote attacker to potentially leak sensitive information via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

84348			
CVE-2026-84840	A vulnerability was identified in tsi-coop tsi-dpdp-cms up to 0.5.0. This affects an unknown part of the file InterceptingFilter.java of the component Bootstrap Setup Endpoint. The manipulation leads to missing authentication. The attack can be initiated remotely. The exploit is publicly available and might be used. Upgrading to version 0.5.1 is able to mitigate this issue. Upgrading the affected component is recommended.	6.5	More Details
CVE-2026-85306	Missing Authorization vulnerability in Cascadia Web Services MountDev AI MCP Connector for WordPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MountDev AI MCP Connector for WordPress: from n/a through 1.6.5.	6.5	More Details
CVE-2026-85787	An incomplete list of disallowed inputs in the SQL validation component in Amazon awslabs postgres-mcp-server before version 1.1.7 might allow an unauthenticated actor to modify data beyond the read-only scope by placing crafted SQL into the content that is submitted when an authenticated user interacts with the MCP server. To remediate this issue, users should upgrade to version 1.1.7 or above.	6.5	More Details
CVE-2026-85703	A flaw has been found in ramon-victor freegpt-webui up to 098db3dfeb41555c2ca9269df0f13e10ec1c35dc. Affected by this issue is the function getJailbreak of the file server/backend.py of the component Jailbreak Mode. Executing a manipulation can lead to allocation of resources. The attack can be executed remotely. The exploit has been published and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. This vulnerability only affects products that are no longer supported by the maintainer.	6.5	More Details
CVE-2026-82052	The $regexFindAll expression can be used by an authenticated user who can run aggregation pipeline stages to crash a MongoDB server (mongod). Under certain specific conditions the regex match can start in the middle of a multi-code-unit character, triggering an assertion during query execution.	6.5	More Details
CVE-2026-77847	Tycon Systems TPDIN-Monitor-WEB3 versions 2.2.9 and prior are vulnerable to a use of hard-coded credential vulnerability. This could allow an attacker to intercept sensitive information or credentials.	6.5	More Details
CVE-2026-53769	Avo is a framework to create admin panels for Ruby on Rails apps. From version 2.28.0 to before version 3.32.0, Avo's direct attachment upload endpoint lacks server-side upload authorization and bypasses the documented field-level upload policy methods such as upload_{FIELD_ID}?. An authenticated Avo user who can reach the Avo attachment upload endpoint can replace or add attachment content, including binary content, filename, and content-type metadata, on a resolved record even when both update? and upload_<field>? policies deny the operation. This primarily affects multi-role Avo Pro/Advanced-style deployments where non-administrator or restricted operator users can reach Avo and per-record or per-field operations are expected to be enforced by policies. This issue has been patched in version 3.32.0.	6.5	More Details
CVE-2026-80129	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to remote execution.	6.5	More Details
CVE-2026-86175	NetBox through 4.7.0 fails to redact sensitive data source backend credentials in REST and GraphQL API responses. Authenticated users with only view permission can retrieve plaintext passwords and secret keys for Git and Amazon S3 backends through API endpoints, gaining unauthorized access to external repositories and storage buckets.	6.5	More Details
CVE-2026-84377	LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to versions 1.88.6 and 1.96.2, any authenticated LiteLLM proxy user could redirect an outbound provider call to a destination the user controls and cause the proxy to send its configured provider credentials to that destination. Request validation in litellm/proxy/auth/auth_utils.py, litellm/proxy/common_request_processing.py, litellm/proxy/health_endpoints/_health_endpoints.py, litellm/proxy/image_endpoints/endpoints.py, and litellm/proxy/litellm_pre_call_utils.py used incomplete checks that did not cover every sensitive parameter or inspect equivalent values across nested request fields, path values, and bracket-notation form data. Routing and credential parameters including api_base, base_url, model_list, fallbacks, and litellm_credential_name could therefore be applied without clearing the operator's stored key, exposing upstream provider credentials and other configured secrets and permitting server-side requests to internal services reachable by the proxy. This issue is fixed in versions 1.88.6 and 1.96.2.	6.5	More Details
CVE-2026-80170	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Use of Hard-coded Credentials vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	6.5	More Details
CVE-2026-86186	AVideo API fails to enforce rate limits when clients send a bot User-Agent header, allowing attackers to bypass all eight protected operations including login brute-force protection. Attackers can send requests with a bot User-Agent to disable rate limiting and perform unlimited password guessing attempts against any account from a single IP address.	6.5	More Details
CVE-	Incorrect authorization in Autofill in Google Chrome on on Android prior to 152.0.7977.75 allowed a remote		

2026-84327	attacker leveraging social engineering to obtain sensitive information via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-85769	A flaw was found in libtpms, a library that provides software TPM 2.0 emulation. When restoring TPM 2.0 state (for example during a virtual machine's power-on or state/migration restore), a malformed state blob can supply an oversized skip-block length that is not validated against the remaining size of the input buffer. This can drive an internal size counter negative, which bypasses a subsequent bounds check due to an unsafe signed-to-unsigned conversion, causing the parser to read memory outside the bounds of the heap buffer holding the state data. Successful exploitation can crash the process hosting libtpms (such as swtpm), resulting in a denial of service of the emulated TPM device and the virtual machine that depends on it. No data corruption or information disclosure was confirmed.	6.5	More Details
CVE-2026-84810	claude-skill-antivirus fails to analyze executable files when scanning local skill directories, reading only SKILL.md while ignoring Python source, bytecode, and other artifacts in the scripts directory. Attackers can distribute skills with malicious code in non-manifest files that receive a SAFE verdict with 100/100 trust score despite containing unanalyzed executable payloads.	6.5	More Details
CVE-2026-85303	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magepeople inc. Booking and Rental Manager allows Stored XSS. This issue affects Booking and Rental Manager: from n/a through 2.7.7.	6.5	More Details
CVE-2026-78488	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	6.5	More Details
CVE-2026-52763	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, the recentchanges action (actions/recentchanges.php) accepts a period argument from two disjoint parameter spaces. A whitelist validates only the URL form against ['day','week','month']. The action-argument form takes the else branch with no validation, and the value flows into PageManager::getRecentlyChanged(), where it is interpolated into a WHERE time >= '...' ORDER BY time DESC clause without escaping or parameterization. UNION-based injection succeeds, the leaked rows render into the response page, so any visitor of the trigger page sees the exfiltrated data. The vulnerability provides arbitrary read of the YesWiki database to anyone who can save the trigger page. On a default install (default_write_acl='*'), this includes anonymous users, subject to the hashcash JS check on the page-edit form. Once the trigger page is saved, every subsequent view fires the injection as the SQLi is stored. Stored SQL injection is reachable through the page-edit flow, with arbitrary database read. This issue has been patched in version 4.6.6.	6.5	More Details
CVE-2026-84971	Improper handling of an unexpected value size in the decryption path of a client-side encryption library can cause a failed internal check that terminates the process using the library. A party able to place a suitably formed encrypted value where an application will decrypt it, or able to control the responses the application receives, may cause that application to stop running.	6.5	More Details
CVE-2026-86116	Metabase versions before 0.63.1 fail to enforce data analyst permission checks on glossary API endpoints, allowing any authenticated user to create, modify, and delete glossary entries. Attackers can submit requests to POST, PUT, and DELETE glossary endpoints to tamper with instance-wide business glossary data without proper authorization.	6.5	More Details
CVE-2026-85044	Use of released resource in Mobile in Google Chrome on on Android prior to 152.0.7977.82 allowed a remote attacker leveraging social engineering to bypass web origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-82299	Incorrect Authorization (CWE-863) in Kibana can lead to information disclosure via Exploiting Incorrectly Configured Access Control Security Levels (CAPEC-180).	6.5	More Details
CVE-2021-43613	An issue was discovered in SysPasswordDxe in Insyde InsydeH2O. User and administrator password hashes are exposed in runtime UEFI variables, leading to escalation of privilege	6.5	More Details
CVE-2026-85389	Worklenz before 3.0.0 fails to verify task ownership by organization when resolving task-scoped API endpoints, allowing authenticated users to access another tenant's task data. Attackers can query task endpoints with arbitrary task UUIDs to retrieve work logs, comments, attachments, and project insights belonging to other organizations.	6.5	More Details
CVE-2022-51015	PocketMine-MP before 4.0.6 does not validate facing values in PlayerActionPacket (for START_BREAK and CRACK_BREAK actions) or in UseItemTransactionData (typically within InventoryTransactionPacket). A remote authenticated attacker can send crafted packets with invalid facing values (e.g., negative or out-of-range) to crash the server, resulting in a denial of service.	6.5	More Details
CVE-	PocketMine-MP before 4.0.7 contains an unhandled exception vulnerability in the ModalFormResponsePacket		More

2022-51014	handler when processing malformed JSON from clients. Attackers can send specially crafted form response packets with invalid JSON to trigger an uncaught InvalidArgumentException, causing server crashes.	6.5	Details
CVE-2022-51013	PocketMine-MP versions before 4.2.3 fail to validate damage metadata values in tool and armor item NBT data received from clients. Attackers can send negative or out-of-range damage values in itemstack NBT to trigger unhandled exceptions in the Durable class, causing server crashes.	6.5	More Details
CVE-2026-86724	AVideo through commit c3edcc274c389816d434acadac07ee78eaf330c1 contains a cross-site request forgery vulnerability in plugin/YPTWallet/view/saveBalance.php that allows attackers to set arbitrary wallet balances by relying only on session cookies without token validation. Attackers can craft a malicious webpage that, when loaded by an administrator, submits a POST request to modify any user's wallet balance to any value.	6.5	More Details
CVE-2022-51012	PocketMine-MP versions before 4.2.9 fail to properly validate NBT data types during deserialization of inventory transaction packets from clients. Attackers can send crafted inventory transactions with malformed NBT tags to trigger server crashes and cause denial of service.	6.5	More Details
CVE-2026-49455	Waku is the minimal React framework. Prior to version 1.0.0-beta.1, Waku's RSC request dispatcher invokes server actions without validating the request's Origin (or Sec-Fetch-Site) header. A cross-origin web attacker can therefore cause a victim browser to issue an authenticated POST to a registered server action endpoint using a CORS-safelisted content type (text/plain), which does not trigger a preflight. Any state-mutating server action that the application exposes via 'use server' can be invoked with the victim's cookies attached. This issue has been patched in version 1.0.0-beta.1.	6.5	More Details
CVE-2026-9745	IBM Netezza Software 11.3.0.3 through Interim Fix 002 has operations that are performed without validating bucket ownership using the ExpectedBucketOwner parameter. This omission may allow a remote attacker to exploit misconfigurations or naming collisions to redirect application requests to an unintended S3 bucket under their control.	6.5	More Details
CVE-2026-84698	PX4 Autopilot contains a heap buffer overflow vulnerability in the sd_bench command that writes a four-byte block number into a user-supplied sized allocation. Attackers can invoke sd_bench with a block size below four bytes to overflow the heap buffer and potentially execute code or crash the system.	6.5	More Details
CVE-2022-51010	PocketMine-MP versions before 4.4.2 fail to properly validate item IDs received from clients in itemstack NBT data. Attackers can send crafted item IDs outside the valid range to trigger an uncaught exception that crashes the server.	6.5	More Details
CVE-2026-86111	BookWyrm through 0.9.1 fails to validate user visibility permissions in the status edit endpoint, allowing authenticated attackers to read followers-only and direct-message reviews by enumerating sequential status IDs. Attackers can access the raw content of restricted statuses through the edit view, bypassing the privacy protections documented for these message types.	6.5	More Details
CVE-2026-82055	A security issue exists in MongoDB's 2dsphere index key generation that can cause a server crash due to a null pointer dereference. When a specially crafted GeoJSON document is inserted into a collection with a 2dsphere index, an inconsistency in geometry parsing can leave an internal object in an invalid, partially initialized state. During subsequent index key generation, access to this improperly initialized object results in a null pointer dereference that terminates the mongod process. An authenticated user with write access can use this to cause a denial of service.	6.5	More Details
CVE-2026-14975	The WP File Download plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.3.8 via the 'remoteurl' parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. An authenticated attacker with Subscriber-level access first poisons the _wpfd_file_metadata['file'] post-meta value via the unprotected file.save handler, after which the streaming endpoint — hooked on init with no authentication requirement — resolves and streams the traversed file path to any caller, including unauthenticated visitors.	6.5	More Details
CVE-2026-86113	BookWyrm through 0.9.1 contains an authorization bypass vulnerability in the edit_readthrough function that allows authenticated users to modify other users' reading records. Attackers can exploit sequential ReadThrough IDs to overwrite arbitrary users' start dates, finish dates, progress, and progress mode, affecting reading statistics and exported data.	6.5	More Details
CVE-2026-86114	Arcane versions before 2.0.0 fail to properly restrict template operations, allowing default user role accounts to create, modify, and delete compose templates including instance-wide defaults. Attackers can inject malicious container configurations with privileged settings or host path mounts that execute with administrative privileges when deployed by administrators.	6.5	More Details
CVE-2026-82054	A security issue exists in MongoDB server's JSON Pointer parser used during $jsonSchema query filter processing. When a find command includes a specially crafted $jsonSchema filter field, the parser processes the input without enforcing adequate limits on iteration count or total allocation size, resulting in significant memory amplification. Under concurrent request load, the cumulative memory consumption can exhaust available heap memory, causing the server's out-of-memory handler to terminate the mongod process and deny service to all connected clients.	6.5	More Details

CVE-2026-86192	SiYuan versions before v3.8.2 fail to properly filter private attribute-view cell values in the getAttributeViewKeys endpoint. Publish readers can retrieve hidden KeyValues payloads from rows bound to inaccessible documents, exposing private database contents without authorization.	6.5	More Details
CVE-2026-85618	ConvertX 0.17.0 contains an arbitrary file read vulnerability in the xelatex converter that allows authenticated users to read files by uploading LaTeX files with input directives. Attackers can upload .tex files containing \\input{path} or \\verbatiminput{path} directives to have the TeX engine read arbitrary files accessible to the server process and include them in downloadable PDF output.	6.5	More Details
CVE-2026-80126	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Locking vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to filesystem access for attacker.	6.5	More Details
CVE-2026-82065	A security issue in the MongoDB Server's storage engine integration layer allows an authenticated user with collection creation privileges to cause a persistent denial of service. Insufficient validation of user-supplied storage configuration options permits values that, once persisted to durable metadata, trigger a fatal assertion failure when the metadata is subsequently read by diagnostic operations. The corrupted metadata persists across server restarts and is replicated to other cluster members, requiring manual operator intervention to restore service.	6.5	More Details
CVE-2026-75793	The SureCart WordPress plugin before 4.7.0 does not consult the site's user registration setting before creating WordPress accounts, allowing unauthenticated users to create an account and receive a logged-in session even when registration is disabled.	6.5	More Details
CVE-2026-81428	The WC Vendors WordPress plugin before 2.7.2.1 does not verify ownership or the object type of user-supplied IDs when saving product variations, allowing authenticated users with the vendor role to modify product variations belonging to other vendors, and to change the status and title of arbitrary posts, via IDOR.	6.5	More Details
CVE-2026-19859	The JetFormBuilder WordPress plugin before 3.6.5.2 does not sanitize a request parameter before rendering it as message content, allowing unauthenticated users to execute arbitrary shortcodes registered on the site on any page displaying a form. Escaping is applied to that content before a later shortcode-expansion pass rather than after it, so the escaping can be bypassed.	6.5	More Details
CVE-2026-17273	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service due to a NULL pointer dereference.	6.5	More Details
CVE-2026-17207	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service and compromise integrity due to a buffer overflow.	6.5	More Details
CVE-2026-17057	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service and affect data integrity due to missing authentication for critical functions.	6.5	More Details
CVE-2026-82068	A security issue in MongoDB Server allows an authenticated user with write privileges to trigger a persistent fatal assertion crash by sending specially crafted retryable write commands. The crash state is durably persisted, causing the server process to repeatedly crash on restart and potentially propagating to additional nodes in a sharded cluster. Manual intervention is required to restore service availability.	6.5	More Details
CVE-2026-86260	A security flaw has been discovered in sfturing hosp_order up to 627f426331da8086ce8fff2017d65b1ddef384f8. The affected element is the function modifyPassWord of the file ssm_pro/src/main/java/cn/sfturing/web/CommonUserController.java of the component Password Recovery. Performing a manipulation results in unverified password change. 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 project was informed of the problem early through an issue report but has not responded yet.	6.5	More Details
CVE-2026-14470	IBM Langflow OSS 1.0.0 through 1.10.2 could allow an authenticated attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	6.5	More Details
CVE-2026-82070	A security issue in MongoDB Server's diagnostic reporting interface allows an authenticated user with monitoring privileges to access insufficiently protected credentials from concurrent administrative operations. The same credentials are properly redacted in server log output, but the diagnostic interface omits equivalent redaction. Successful exploitation requires a valid authenticated session with monitoring-level permissions and results in exposure of cleartext credentials that could enable impersonation of other users, including privileged accounts.	6.5	More Details
CVE-2020-37277	PocketMine-MP versions before 3.15.4 contain a denial of service vulnerability in the InventoryTransaction component's findResultItem() method. Malicious clients can send specially crafted InventoryTransactionPackets with multiple conflicting pathways to cause exponential processing complexity, freezing the server.	6.5	More Details

CVE-2021-48007	PocketMine-MP versions before 3.18.1 fail to validate NaN or INF values in MovePlayerPacket position and rotation fields. Malicious clients can send crafted movement packets with invalid floating-point values to crash servers through unhandled mathematical operations or prevent clients from rendering other players.	6.5	More Details
CVE-2026-44766	SAP S/4HANA (Intercompany Matching and Reconciliation) allows a low-privileged authenticated user to inject malicious input into certain functions, which may be processed by the database without proper validation. This could allow the user to access sensitive information, resulting in high impact on confidentiality, with no impact on integrity and availability of the application.	6.5	More Details
CVE-2026-84811	agentverus-scanner fails to analyze compiled Python bytecode files in companion code directories, allowing attackers to bypass security scanning by shipping malicious __pycache__ entries alongside benign source files. Attackers can execute arbitrary Python bytecode on import while the scanner reports a CERTIFIED verdict with high trust scores in both static and semantic analysis modes.	6.5	More Details
CVE-2026-84781	Contributor Cross Site Scripting (XSS) in Gallery PhotoBlocks <= 1.3.4 versions.	6.5	More Details
CVE-2026-76968	SAP Web Dispatcher, Internet Communication Manager and SAP Content Server allows an authenticated low-privileged attacker to access certain administrative functionality or interface and obtain sensitive information about the system state, resulting in information disclosure. This disclosed information could potentially be used to facilitate further attacks. This vulnerability has a high impact on the confidentiality of the application, with no impact on integrity or availability.	6.5	More Details
CVE-2026-76971	Due to a Server-Side Request Forgery (SSRF) vulnerability in SAP Manufacturing Integration and Intelligence, an attacker could cause the server to initiate arbitrary outbound requests. If processed by the application, this behavior could be combined with XML/XSL processing to enable execution of scripts. Successful exploitation could result in a low impact on the confidentiality, integrity, and availability of the application.	6.5	More Details
CVE-2026-86255	wger before 2.5 fails to validate the maximum duration of routine date ranges, allowing authenticated users to create routines spanning arbitrarily long periods. Attackers can trigger the date_sequence computation via routine detail endpoints, forcing the server to iterate thousands of times per request and exhaust worker threads, denying service to legitimate users.	6.5	More Details
CVE-2026-82073	A security issue in the MongoDB Server aggregation framework allows an authenticated user with limited read privileges to bypass view-level authorization checks and access data from unauthorized collections when Atlas Search features are in use. The issue stems from insufficient validation of an internal command parameter that can be set by external clients, causing a security check to be improperly skipped.	6.5	More Details
CVE-2026-84357	Improper input validation in Omnibox in Google Chrome prior to 152.0.7977.75 allowed a remote attacker leveraging social engineering to bypass web origin policy via crafted network traffic. (Chromium security severity: High)	6.5	More Details
CVE-2026-17622	IBM Langflow OSS 1.0.0 through 1.10.2 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	6.5	More Details
CVE-2026-82058	A flaw in MongoDB's JSON Schema validation error generation code allows an authenticated user with readWrite privileges to crash the mongod server. When a BSON document containing an array with a malformed numeric field name fails a $jsonSchema items type constraint, the error generation path performs unsafe numeric conversion on the user-controlled field name without proper exception handling, resulting in an uncaught exception that terminates the server process. This is possible because incoming wire protocol BSON validation does not enforce that array element field names are valid, in-range numeric indices.	6.5	More Details
CVE-2026-86489	In JetBrains YouTrack before 2026.2.18634 an IDOR in the user profile API disclosed private issues and starred folders across organizations	6.5	More Details
CVE-2026-84391	A use of uninitialized variable vulnerability in Fortinet FortiAnalyzer 7.6.3 through 7.6.6 may allow attacker to denial of service via <insert attack vector here>	6.5	More Details
CVE-2026-86493	In JetBrains YouTrack before 2026.2.18634 improper permission checks allowed read-only users to create and modify whiteboard cards	6.5	More Details
CVE-2026-86488	In JetBrains YouTrack before 2026.2.18634 iDOR via the watchRules and issueListConfig endpoints exposed private saved searches	6.5	More Details
	A flaw was found in odh-dashboard in Red Hat OpenShift AI. The backend-for-frontend route GET /api/nim-serving/:nimResource reads Kubernetes Secrets using the dashboard service account and returns the full		

CVE-2026-86332	Secret object, including .data, without an authorization check. Any authenticated dashboard user can retrieve the cluster NVIDIA NGC API key Secret (apiKeySecret) and the NIM image pull secret (nimPullSecret). Create and delete of the same NIM credential are admin-gated; the read path is not. This is missing authorization (CWE-862) and insufficiently protected credentials (CWE-522). It is distinct from CVE-2026-5483 (service-account token leak in the Kubernetes client response wrapper on the same route) and CVE-2026-16456 (odh-model-controller cross-namespace confused deputy).	6.5	More Details
CVE-2026-86726	AVideo through 29.0 contains an information disclosure vulnerability in restreamsActive.json.php that allows authenticated streamers to enumerate source stream keys and identities of all other streamers' active restreams. The endpoint fails to filter results by user ownership, exposing sensitive transmission credentials and streamer identity across all accounts to any user with streaming capability.	6.5	More Details
CVE-2026-61688	SolidInvoice is an open-source invoicing platform. Prior to version 3.0.1, an authenticated user can view the API request history of any other user's API tokens within the same company by manipulating two writable Symfony UX LiveComponent props on the `DataGrid` component. Version 3.0.1 fixes the issue.	6.5	More Details
CVE-2026-84849	Unauthenticated Bypass Vulnerability in Pre-Orders for WooCommerce <= 2.3 versions.	6.5	More Details
CVE-2026-86293	A flaw has been found in SourceCodester Simple Traffic Offense System 1.0. Affected by this vulnerability is an unknown functionality of the file delete-user.php of the component Deletion Endpoint. Executing a manipulation of the argument ID can lead to missing authentication. The attack may be launched remotely. The exploit has been published and may be used.	6.5	More Details
CVE-2026-86490	In JetBrains YouTrack before 2026.2.18634 improper permission checks allowed overwriting of bundled apps via the app import endpoint	6.5	More Details
CVE-2026-82057	A security issue was discovered in MongoDB where an authenticated user with readWrite privileges could crash the mongod server process. By specifying a custom WiredTiger storage configuration option with an incompatible value during collection creation, a user could cause a type confusion in the storage engine layer. When documents were subsequently read from the misconfigured collection, the resulting mismatch in expected data format led to corrupted memory interpretation and a server crash. The crafted collection configuration persists across restarts, requiring manual operator intervention to remediate.	6.5	More Details
CVE-2026-2688	The HIPAA FORMS WordPress plugin before 3.2.0 contains a hardcoded authentication bypass via a hardcoded parameter alongside all AJAX requests. The server explicitly checks for this value to skip nonce validation entirely. This allows unauthenticated attackers to access protected AJAX endpoints.	6.5	More Details
CVE-2026-84332	Incorrect authorization in SiteSettings in Google Chrome prior to 152.0.7977.75 allowed a remote attacker to bypass system access restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-85302	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPKoi WordPress Themes WPKoi Templates for Elementor allows DOM-Based XSS. This issue affects WPKoi Templates for Elementor: from n/a through 3.7.2.	6.5	More Details
CVE-2026-84933	undici's cache interceptor does not handle the Set-Cookie response header anywhere in its cache path, so it neither refuses to store nor strips that header. In shared cache mode, which is the default, an otherwise cacheable response that carries a Set-Cookie header, for example one marked with a public and max-age directive, is stored and then re-served to a later caller that matches the same cache key. As a result one caller's cookie is disclosed to a different caller, and an untrusted server can inject cookies into cached responses served to all subsequent callers. This violates the requirement that a shared cache must not store cookies. This affects undici versions from 7.0.0 up to 7.29.1 and from 8.0.0 up to 8.10.2. Users should upgrade to undici 7.29.1 or 8.10.2.	6.5	More Details
CVE-2026-86495	In JetBrains YouTrack before 2026.2.18687 missing permission checks allowed creating knowledge base articles in inaccessible projects	6.5	More Details
CVE-2026-3850	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `redirect_url` parameter of the `et_pb_contact_form` shortcode in all versions up to, and including, 4.27.6. This is due to the `redirect_url` attribute being sanitized with `esc_attr()` instead of `esc_url()` before being rendered into the `data-redirect_url` HTML data attribute. Additionally, `redirect_url` is absent from the hardcoded `$url_options` array in `class-et-builder-element.php`, so it does not receive `esc_url_raw()` sanitization during shortcode parsing. After a successful form submission, client-side JavaScript reads this data attribute and passes it directly to `window.location.href`, executing arbitrary JavaScript from a `javascript:` URI. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that execute whenever a user submits the contact form.	6.4	More Details
CVE-	The Easy Waveform Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the shortcode_easywaveformplayer() function in all versions up to, and including, 1.2.2 due to insufficient input		

2025-7963	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-2026-83534	PostgreSQL Anonymizer contains a vulnerability in the anon.anonymize_database_parallel() function that allows the owner of a table to run arbitrary code with superuser privilege. The issue is fixed in PostgreSQL Anonymizer 3.2.0 and later versions	6.4	More Details
CVE-2026-12230	The LearnPress – WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'layout_custom_css' parameter in all versions up to, and including, 4.3.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-80128	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Authentication vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	6.4	More Details
CVE-2026-85414	The Gallery : FooGallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'custom_settings' Shortcode Attribute in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-76573	The Pods – Custom Content Types and Fields plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'not_found' Shortcode Attribute in all versions up to, and including, 3.3.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3851	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting via the Dynamic Content feature's legacy JSON format in all versions up to, and including, 4.27.6. This is due to two compounding flaws: (1) the save-time sanitization filter `et_builder_sanitize_dynamic_content_fields()` only searches for dynamic content markers in the `@ET-DC@...@` format, but the rendering engine also supports a legacy JSON format that is silently converted at render time, completely bypassing the save-time filter, and (2) the `post_meta_key` resolver in `et_builder_filter_resolve_default_dynamic_content()` does not apply `wp_kses_post()` to the resolved meta value when `enable_html` is set to `on`, passing raw `get_post_meta()` output directly to the page. 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-2026-3853	The Divi theme for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the `image_src` attribute of the `et_pb_video_slider_item` shortcode in all versions up to, and including, 4.27.6. This is due to the `image_src` field not being included in the `$url_options` whitelist (which only contains `url`, `button_link`, `button_url`), so it never receives `esc_url_raw()` at save time. On the server side, the value is rendered into a `data-image` HTML attribute using `esc_attr()`, which encodes double quotes as `"`. However, the client-side JavaScript carousel code in `custom.unified.js` reads this attribute using jQuery's `.data('image')`, which returns the browser-decoded value (with `"` decoded back to `"`). The decoded value is then concatenated directly into an HTML string and injected into the DOM via `jQuery.after()` without re-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 hovers over the carousel thumbnail.	6.4	More Details
CVE-2026-8625	The Dear Flipbook – PDF Flipbook, 3D Flipbook, PDF embed, PDF viewer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_content (Custom HTML block inner HTML)' parameter in all versions up to, and including, 2.4.30 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. A Contributor-level attacker can insert a crafted .df-element div with data-df-lightbox='thumb' via a Custom HTML block, whose inner HTML is passed as the title argument to parseThumbs() at render time, enabling both innerHTML injection into a span element and attribute breakout via an onerror handler on a constructed img element.	6.4	More Details
CVE-2026-8623	The Dear Flipbook – PDF Flipbook, 3D Flipbook, PDF embed, PDF viewer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_content (class attribute of .dvcss element)' parameter in all versions up to, and including, 2.4.30 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 payload is embedded as a Base64-encoded JSON object in a CSS class name on a Custom HTML block; the frontend parseCSSElements() function decodes it client-side with atob() and JSON.parse() and renders the logo property as raw HTML, meaning no server-side or client-side sanitization intercepts the malicious script before DOM insertion.	6.4	More Details
	The Social Chat – Click To Chat App Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'consent_message' JSON Attribute in .qlwapp data-box in all versions up to, and including, 8.6.2 due to		

CVE-2026-18404	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 requires no user interaction beyond page load, as setting auto_open and consent_enabled to 'yes' in the injected data-box JSON causes the consent box — and the embedded script — to execute immediately on page load.	6.4	More Details
CVE-2026-86100	Camaleon CMS versions 2.7.5 through 2.9.1 fail to validate redirect targets when fetching remote files in the Upload from URL media feature. Authenticated attackers can supply URLs that pass initial validation but redirect to internal network addresses, allowing server-side request forgery to internal services.	6.4	More Details
CVE-2026-19634	PostgreSQL Anonymizer contains a SQL injection vulnerability in two import functions. A user can create a malicious JSON document containing specially crafted object names. If a superuser subsequently calls anon.import_database_rules() or anon.import_roles_rules(), the malicious code is executed with superuser privileges. The issue is fixed in PostgreSQL Anonymizer 3.1.4 and later	6.4	More Details
CVE-2026-76931	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘message’ parameter in all versions up to, and including, 3.3.205 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. The vulnerability can only be exploited when the 'Directly link to project' plugin setting is disabled.	6.4	More Details
CVE-2026-82968	A flaw was found in the first-broker-login flow of the Keycloak identity management service. When a user links a social identity provider account to their local account, the verification proof generated is not strictly bound to the specific upstream identity being verified. This allows an attacker with a different account on the same social provider to intercept the process and link their own account to the victim's local profile, gaining unauthorized access.	6.4	More Details
CVE-2026-85615	Openpanel before 2.3.0 contains an insecure direct object reference vulnerability in the report.getLayouts and report.resetLayout tRPC procedures that fail to bind dashboardId to the authorized projectId. Authenticated attackers can supply an arbitrary victim dashboardId with their own projectId to read report layouts and configurations or delete dashboard grid arrangements across tenants.	6.4	More Details
CVE-2026-3852	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `skype_url` shortcode attribute of the Social Media Follow module in all versions up to, and including, 4.27.6. This is due to a three-part sanitization failure: (1) the `skype_url` field is not included in the `$url_options` whitelist in `class-et-builder-element.php`, so it never invokes `esc_url_raw()` during shortcode processing, (2) the render code in `SocialMediaFollowItem.php` explicitly skips `esc_url()` for Skype URLs (`! $is_skype ? esc_url( $url ) : $skype_url`), and (3) only `sanitize_text_field()` is applied, which preserves single and double quote characters allowing attribute breakout. The unsanitized value is interpolated directly into a single-quoted `href` attribute (`href='{$social_network_link_url}'`). 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 interacts with the injected element.	6.4	More Details
CVE-2026-2573	The GutenKit – Page Builder Blocks, Patterns, and Templates for Gutenberg Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘postBodyCss’ parameter in all versions up to, and including, 2.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2390	The Powerkit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Lazy Load module's image processing in all versions up to, and including, 3.0.4. This is due to the 'content_process_images' function using a flawed regex-based HTML attribute parser. 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-2026-85611	OpenPanel before 2.3.0 contains a cross-tenant broken object level authorization vulnerability in the report.getLayouts and report.resetLayout tRPC procedures that fail to scope dashboard queries to the caller's project. Authenticated attackers can supply their own projectId with a victim organization's guessable dashboardId to read confidential report definitions or permanently delete dashboard layouts across tenant boundaries.	6.4	More Details
CVE-2026-85598	Grav versions 2.0.0 through 2.0.17 fail to apply save-time XSS detection to modular pages, allowing authenticated page editors to store Twig-assembled XSS payloads. Attackers with page-edit rights can create modular pages with malicious Twig code that executes in visitor browsers when the parent page is rendered, including in administrator sessions.	6.4	More Details
CVE-2026-75134	SEOWriting plugin for WordPress through 1.12.5 contains a stored cross-site scripting vulnerability that allows authenticated contributors to inject malicious JavaScript by exploiting an overly permissive KSES allowlist that explicitly permits the onload event handler on iframe elements. Attackers can store crafted JavaScript payloads in post content that execute when the affected post is viewed or previewed by higher-privileged users, potentially leading to privilege escalation or account compromise.	6.4	More Details
	A vulnerability was detected in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is		

CVE-2026-86245	an unknown functionality of the file /pages/sup_transac.php. Performing a manipulation of the argument companyname results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-86269	A flaw has been found in itsourcecode Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/emp_edit1.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-86514	A weakness has been identified in vgmstream up to r2117. This issue affects the function sscanf of the file src/meta/txth.c of the component txth-txtp. This manipulation causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. Patch name: 4669d37a6af94866f6f0628678f9f90d46954e8b. To fix this issue, it is recommended to deploy a patch.	6.3	More Details
CVE-2026-86512	A vulnerability was identified in java-json-tools json-patch up to 1.13. This affects the function CopyOperation.apply/MoveOperation.apply of the file src/main/java/com/github/fge/jsonpatch/CopyOperation.java of the component Copy Move Operations. The manipulation leads to improper access controls. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-86518	A vulnerability has been found in code-projects Student Crud Operation 1.0. This affects an unknown function of the file /edit.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-6217	Use of a One-Way hash without a salt vulnerability in Pik Online Software Solutions Inc. Pik Online Portal allows Cryptanalysis. This issue affects Pik Online Portal: through 3.5.1.	6.3	More Details
CVE-2026-86310	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/cust_edit1.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-85513	A weakness has been identified in StackStorm st2 up to 3.9.0. This issue affects the function assert_user_is_admin_if_user_query_param_is_provided of the file st2api/st2api/controllers/v1/actionexecutions.py of the component NoOp RBAC backend. This manipulation of the argument User causes improper privilege management. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. Prior advisory CVE-2022-44009 was reported as a follow-up on the same sink, but this issue is distinct: it needs no Jinja RBAC und affects default install with RBAC disabled. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-86517	A flaw has been found in itsourcecode Sales and Inventory System 1.0. The impacted element is the function mysqli_query of the file /pages/us_searchfrm.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-85135	A security flaw has been discovered in ILIAS up to 9.21/10.9/11.2. This affects the function ilObjMediaObjectGUI::uploadMultipleSubtitleFileObject of the file Services/Repository/Service/Resources/ZipAdapter.php of the component MediaPool. The manipulation results in unrestricted upload. The attack may be launched remotely. Upgrading to version 9.22, 10.10 and 11.3 is able to mitigate this issue. The patch is identified as ef5d7f99fe1ea0381db04b333a2906548b3590e4/b0d61be43671b6bfe91baf469a5ee11e764f2e23. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-85241	A weakness has been identified in SpecterOps BloodHound up to 9.5.1. The affected element is the function NewV2API of the file cmd/api/src/api/registration/v2.go of the component Graph Write Endpoint. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. Upgrading to version 9.6.0-rc1, 9.6.0 and 9.7.0-rc3 is sufficient to fix this issue. This patch is called 39d1276a63e95a7713f954dea632a19651d9cebb. You should upgrade the affected component.	6.3	More Details
CVE-2026-86267	A security vulnerability has been detected in itsourcecode Information System Society Membership System 1.0. This issue affects some unknown processing of the file /society/check_student.php. The manipulation of the argument student_id leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-78591	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) in the Kibana Fleet feature can lead to the unauthorized deletion of resources via Path Traversal (CAPEC-126). A low-privileged user could cause a subsequent action taken by a higher-privileged user in the Fleet administration interface to act on an unintended target, resulting in the deletion of resources including accounts with elevated privileges.	6.3	More Details

CVE-2026-85084	Out-of-bounds Write and Improper Validation of Array Index vulnerability in Samsung Open Source TizenFX Samsung/TizenFX allows Overflow Buffers.	6.3	More Details
CVE-2026-86279	A vulnerability was determined in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. The impacted element is an unknown function of the file auth_process.php of the component Login. This manipulation causes session fixiation. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-75168	An issue in the ugw-editfile method of /cgi-bin/wwwugw.cgi in MBS-Solutions X-Serie Gateway firmware V6_00_05 allows a remote authenticated user with the low-privileged Standard role to write arbitrary content to files within /uxx/config/ and /ugw/config/.	6.3	More Details
CVE-2026-86270	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. The impacted element is an unknown function of the file /pages/settings_edit.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-86232	A weakness has been identified in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/sup_del.php?type=supplier. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-86233	A security vulnerability has been detected in itsourcecode Sales and Inventory System 1.0. Affected by this issue is some unknown functionality of the file /pages/us_del.php?type=user. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-86234	A vulnerability was detected in itsourcecode Sales and Inventory System 1.0. This affects an unknown part of the file /pages/cust_transac.php?action=add. The manipulation of the argument firstname results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-86235	A flaw has been found in itsourcecode Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/pos_transac.php?action=add. This manipulation of the argument Customer causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-85514	A security vulnerability has been detected in StackStorm st2 up to 3.9.0. Impacted is an unknown function of the file st2api/st2api/controllers/v1/auth.py of the component API Key Handler. Such manipulation of the argument api_key_api.user leads to improper privilege management. The attack may be performed from remote. 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-2026-86309	A flaw has been found in itsourcecode Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/pro_searchfrm.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-86170	A weakness has been identified in DefaultFuction CRM 1.0.0. The impacted element is an unknown function of the file /modules/orders/edit.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-18341	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to corrupt memory due to an integer underflow.	6.3	More Details
CVE-2026-85383	A flaw has been found in itsourcecode Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/inv_del.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-84430	A security vulnerability has been detected in gouguoa up to 5.10.0/6.0.1. This vulnerability affects the function update of the file app/home/controller/Index.php of the component edit_personal Endpoint. Such manipulation of the argument position_id leads to dynamically-determined object attributes. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 6.0.3 is able to resolve this issue. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-85401	A weakness has been identified in Dolibarr up to 21.0.4/22.0.5/23.0.3. Affected by this issue is some unknown functionality of the file htdocs/core/filemanagerdol/connectors/php/config.inc.php of the component Legacy File Manager. Executing a manipulation can lead to improper access controls. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 23.0.4 can resolve this issue. This patch is called ef6631e9bd5ec4b8cec0e88f1796d3d10dad02ec. It is suggested to upgrade the affected component.	6.3	More Details
CVE-	A vulnerability was determined in itsourcecode Online Medicine Delivery System 1.0. This issue affects the		

2026-85205	function addwishlist of the file /customer/controller.php?action=addwish of the component Wishlist. This manipulation of the argument proid causes sql injection. The attack may be initiated remotely.	6.3	More Details
CVE-2026-86291	A security vulnerability has been detected in itsourcecode Sales and Inventory System 1.0. This impacts an unknown function of the file /pages/us_edit1.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2026-85186	A weakness has been identified in itsourcecode Online Medicine Delivery System 1.0. Affected by this vulnerability is the function doupdateimage of the file /customer/controller.php?action=photos of the component Customer Controller. Executing a manipulation of the argument photo can lead to unrestricted upload. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-86163	A vulnerability was identified in itsourcecode Sales and Inventory System 1.0. This impacts an unknown function of the file /pages/pro_del.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-86164	A security flaw has been discovered in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/trans_view.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-85409	A vulnerability was identified in Eleveo Quality Management 9.7.0. The affected element is the function QuestionnaireService.runDataExportNow of the component Questionnaire Service. Such manipulation of the argument file_name leads to path traversal. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-77697	Zohocorp ManageEngine Endpoint Central versions below 11.4.2540.23 are vulnerable to Privilege Escalation During JAR Extraction	6.3	More Details
CVE-2026-84797	Craft CMS versions before 5.10.11 contain an authorization bypass vulnerability in ElementsController::actionDuplicate() that allows authenticated users with createEntries permission to delete peer provisional drafts. Attackers can exploit the deleteProvisionalDraft parameter to delete another user's unsaved draft without proper authorization checks, gaining access to the victim's in-progress content.	6.3	More Details
CVE-2026-86171	A security vulnerability has been detected in DefaultFuction CRM 1.0.0. This affects an unknown function of the file /modules/orders/delete.php. Such manipulation of the argument 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-2026-86172	A vulnerability was detected in DefaultFuction CRM 1.0.0. This impacts an unknown function of the file /modules/customers/delete.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-86236	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. This issue affects some unknown processing of the file /pages/pro_transac.php?action=add. Such manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-85106	A vulnerability has been found in NousResearch hermes-agent 0.18.0. This affects the function fetchLinkTitle of the file apps/desktop/src/app/artifacts/index.tsx of the component Link Title Fetch. Such manipulation of the argument url leads to server-side request forgery. The attack can be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-86265	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/us_transac.php. Such manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-84651	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the REST API and CLI endpoints for updating agent configuration do not prevent a submitted configuration from overwriting a different agent by specifying that agent's name in the submitted XML document, allowing attackers with Agent/Configure permission on one agent to take over a different agent, gaining control of its configuration and obtaining access to its inbound agent secret and environment variables.	6.3	More Details
CVE-2026-85640	Zohocorp ManageEngine Endpoint Central versions below 11.5.2600.15 are vulnerable to Privilege Escalation Due to Outdated Component	6.3	More Details
CVE-	A vulnerability has been found in ModelCloud GPTQModel up to 7.2.0. This vulnerability affects unknown code of the file gptqmodel/nn_modules/qlinear/tritonv2.py of the component Triton dequantization kernel. Such		

2026-86288	manipulation of the argument g_idx leads to out-of-bounds read. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 7.3.0 is able to resolve this issue. The name of the patch is 877c732f7d7dccd56a729844c6a5bd20f3aa8bb1. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-16689	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a local attacker to obtain sensitive information due to improper logging of credentials.	6.2	More Details
CVE-2026-84970	A numeric truncation weakness exists in the JSON parsing component of the MongoDB C++ Driver's BSON library. An actor who controls the text that an embedding application hands to the library's public JSON parsing interface, when that text is very large, can cause the library to read memory beyond the supplied buffer and return it to the caller, to silently accept only part of the input as a complete document, or to terminate the process. No MongoDB server, credentials, or non-default configuration is required; the effect is confined to the process that uses the library.	6.2	More Details
CVE-2026-86315	An out-of-bounds write caused by numeric truncation Samsung Open Source Escargot on Linux x86-64 allows an attacker who can supply JavaScript for execution to corrupt native memory and crash the host process via a crafted class definition whose instance initialization entry count exceeds UINT16_MAX. This issue affects Escargot: 5dc93606abd42b859045add05d704a038e197359.	6.2	More Details
CVE-2026-19649	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a local attacker to obtain sensitive information due to improper logging of database credentials.	6.2	More Details
CVE-2026-81859	CP4BA - IBM Enterprise Records could allow a local attacker to obtain sensitive information due to the use of a broken or risky cryptographic algorithm.	6.2	More Details
CVE-2026-19795	Qiskit could allow a local attacker to cause a denial of service due to a stack overflow during deserialization of QPY payloads. A malicious QPY payload can trigger a segmentation fault, causing the application to crash when deserializing untrusted input.	6.2	More Details
CVE-2026-71429	stream-json is a micro-library of stream components for processing JSON and JSONC with a minimal memory footprint. Prior to 3.5.0, the path filters pick, ignore, filter, and replace in src/core/filters/filter-base.js recompute the full path string from the nesting stack for every checkable token. Because the stack length equals the current nesting depth and a checkable token is emitted at every level, a depth D document costs $O(D^2)$ rather than O(D) to process. The issue is triggered by nesting depth rather than byte volume, including the documented pick({filter: 'data'}) traversal-until-match path, so an application that sends untrusted JSON through a string or RegExp filter can block the Node.js event loop and cause denial of service with a small deeply nested document. The streamArray, streamObject, and streamValues streamers are not affected because they use the constant-time asm.depth getter. This issue is fixed in version 3.5.0.	6.2	More Details
CVE-2026-86314	Integer overflow in the source-bounds check in Memory::init() (src/runtime/Memory.cpp) in Samsung walrus on all platforms allows a remote attacker to cause an out-of-bounds heap read and denial of service via a crafted WebAssembly module in which a 32-bit unsigned addition wraps around and bypasses the bounds check. This issue affects Walrus: ff3bf5ff5c4878f8e5572c9593d303f6bc997443.	6.2	More Details
CVE-2026-75137	UpSignOn for Windows before 7.19.0 contains a sensitive data exposure vulnerability that allows local attackers to recover cleartext vault data from process memory even after the application has been locked. Attackers can use the PROCESS_VM_READ permission to read the memory space of UpSignOn.exe and extract sensitive fields including entry names, URLs, usernames, passwords, TOTP secrets, and notes.	6.1	More Details
CVE-2026-75136	UpSignOn for Windows before 7.19.0 contains an insecure credential storage vulnerability that allows local attackers to retrieve the biometric unlock key stored in the Windows PasswordVault API without triggering any authentication prompt. Attackers can access the stored biometric key from a standard local process within the same Windows session to decrypt the protected vault files and export the entire password manager contents in cleartext.	6.1	More Details
CVE-2026-32773	There is a lack of XSS escaping in the Spark History Server prior to 3.5.8 which allows a malicious Spark job to generate arbitrary unescaped frontend code which could lead to a minimal privilege escalation in browser. Users are encouraged to upgrade to Spark 3.5.8 or later. This CVE is marked as "low" since the path to exploit requires both relatively high permissions (ability to launch a Spark job) and requires tricking a user with higher permissions to log in and visit the Spark history web page. Users are encouraged to upgrade their Spark history servers to Spark 3.5.8 or later.	6.1	More Details
CVE-2026-80180	Stored XSS via markdown HTML processing in Apache Allura. This issue affects Apache Allura: from through 1.20.0. Users are recommended to upgrade to version 1.21.0, which fixes the issue.	6.1	More Details
CVE-2026-85229	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Apache SkyWalking Booster UI. This issue affects Apache SkyWalking UI : from 10.2.0 through 10.4.0. Users are recommended to upgrade to Horizon UI 1.0.0, which fixes the issue.	6.1	More Details

CVE-2026-75135	UpSignOn for Windows before 7.19.0 contains a sensitive data exposure vulnerability that allows local attackers to recover the master password and decrypt vault contents by reading a retained backup key from the process memory of UpSignOn.exe, even after the vault has been re-locked. Attackers can extract the backup key from process memory to decrypt the encrypted master password backup stored in v6-vault1.DATA.txt, then use the recovered master password to decrypt the main vault and export all password manager entries in cleartext.	6.1	More Details
CVE-2026-85453	MOOS core-moos through 10.4.0 fails to escape database contents when rendering MOOSDB HTTP pages, allowing attackers to inject malicious scripts. Any MOOS publisher can set variable values containing script payloads that execute in the browser of operators viewing the web interface.	6.1	More Details
CVE-2026-52774	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, YesWiki's Bazar widget handler reflects the id GET parameter into HTML attributes using strip_tags() only. Because strip_tags() does not escape double quotes, an attacker can break out of the attribute value, inject an event handler such as onmouseover, and execute arbitrary JavaScript in the victim's browser. This issue is reachable without authentication. During validation, the vulnerable widget route returned the injected HTML for both /HomePage/widget?id=... and /NoSuchPage/widget?id=..., which shows that no login, no page ownership, no edit rights, and not even a valid page tag were required. The only routing prerequisite observed was that the Bazar extension is enabled and the request includes an id parameter. This issue has been patched in version 4.6.6.	6.1	More Details
CVE-2026-80190	Apache Allura: stored XSS via SVN code repositories. Git repositories are not known to be affected. The vulnerability is likely mitigated via default CSP headers. This issue affects Apache Allura: through 1.20.0. Users are recommended to upgrade to version 1.21.0, which fixes the issue.	6.1	More Details
CVE-2026-52773	YesWiki is a wiki system written in PHP. From version 4.1.0 to before version 4.6.6, YesWiki's archived-revision view reflects the time GET parameter into a hidden HTML input in handlers/page/show.php without escaping. Because MySQL coerces malformed DATETIME strings, an attacker can append HTML or JavaScript to a valid archived revision timestamp, still load that archived revision, and execute arbitrary JavaScript in the victim's browser. The vulnerable form is only rendered when the victim can both read and edit the target page. In restricted deployments this requires a victim with read and write access to that page. On a default doryphore 4.6.5 install, public pages such as PagePrincipale were editable anonymously during validation, so the issue can also affect unauthenticated visitors in that configuration. This issue has been patched in version 4.6.6.	6.1	More Details
CVE-2026-80115	PassMark PerformanceTest before 11.1 build 1012, BurnInTest before 11.1 build 1000, and OSForensics before 11.1 build 1016 contain a privilege escalation and denial-of-service vulnerability in DirectIo64.sys that allows local attackers to read arbitrary Model-Specific Registers or write zero to any MSR through exposed IOCTLs with insufficient blocklist enforcement. Attackers can exploit the unrestricted write IOCTL to zero out the system call handler MSR, causing an immediate unrecoverable kernel crash on the next system call, or read security-sensitive MSRs used to locate kernel data structures.	6.1	More Details
CVE-2026-81160	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Slick Carousel allows Stored XSS. This issue affects Slick Carousel versions: from 0.0.0 to 2.1.0.	6.1	More Details
CVE-2026-85454	MOOS core-moos through 10.4.0 contains a buffer overflow vulnerability in CMOOSSerialPort::GetTelegram() that writes a NUL terminator one byte past the serial telegram stack buffer. Attackers controlling the serial line can send a full-length telegram to trigger the off-by-one write, corrupting the stack and potentially enabling code execution.	6.1	More Details
CVE-2026-84774	Unauthenticated Cross Site Scripting (XSS) in WP Statistics <= 14.16.11 versions.	6.1	More Details
CVE-2026-81201	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Monster Menus allows Stored XSS. This issue affects Monster Menus versions: from 0.0.0 to 9.5.3.	6.1	More Details
CVE-2026-58113	A vulnerability has been identified in Teamcenter V2412 (All versions < V2412.0013), Teamcenter V2506 (All versions < V2506.0010), Teamcenter V2512 (All versions < V2512.2607), Teamcenter V2606 (All versions < V2606.2607). Affected applications do not properly encode user-supplied input reflected into HTML attribute contexts within the authentication redirect flow (/auth/ endpoint). This could allow an unauthenticated remote attacker to inject arbitrary JavaScript into the browser of an authenticated user who loads a crafted URL, enabling the attacker to perform actions within the victim's Teamcenter session.	6.1	More Details
CVE-2026-71403	A flaw was found in Rancher Manager. The /v3/users update path did not enforce immutability of a User resource's `username` and `principalIds` fields. A user holding the `update` verb on `users.management.cattle.io` could inject a foreign identity provider principal into any account, so that the next login by the owner of that principal was bound to the victim's account and inherited its role bindings. This issue affects Rancher: before 2.15.1.	6.1	More Details

CVE-2026-8447	IBM Langflow OSS 1.0.0 through 1.11.2 suffer from a stored cross-site scripting vulnerability in the Playground chat interface.	6.1	More Details
CVE-2026-73319	XenForo before 2.3.13 contains a cross-site scripting vulnerability in the dynamic redirect handler that allows unauthenticated attackers to execute arbitrary JavaScript in the board origin by crafting a malicious javascript: URI that bypasses host validation. Attackers can embed the board hostname in the URI authority component and use percent-encoded newlines to evade server-side filters, causing authenticated users who perform a Follow action to execute attacker-supplied JavaScript in their browser.	6.1	More Details
CVE-2022-51016	PocketMine-MP 3.x (before 3.27.0) does not implement Minecraft Bedrock protocol encryption, so the server cannot verify that a connecting client possesses the private key corresponding to its login token. An attacker who captures a valid login from another player's session (for example by tricking the player into connecting to an attacker-controlled server) can replay that login to impersonate the victim and pass XBOX Live authentication until the JWT token expires (typically 2-3 days). This affects servers directly reachable over the internet that are not behind a proxy with encryption enabled. Fixed in 4.0.0 and backported to 3.27.0.	6.1	More Details
CVE-2026-75586	The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 'formData[id]' Parameter in all versions up to, and including, 2.0.17 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. The front-end AJAX handler is registered on the public 'wp' action with no nonce, capability, or referer check, and the raw attacker-controlled id value is interpolated verbatim into an exception message that is echoed back without escaping; when the response is served as text/html rather than application/json, the browser parses the injected markup.	6.1	More Details
CVE-2026-18843	The Beaver Builder Plugin (Starter Version) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 'no_results_message' node_preview Parameter in all versions up to, and including, 2.11.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-73320	XenForo before 2.3.13 contains an unauthenticated information disclosure vulnerability that allows unauthenticated attackers to retrieve private unfurl records by supplying predictable auto-increment primary key IDs to the unfurl endpoint. Attackers can enumerate or predict result IDs and query the endpoint without any session, user, or visibility checks to obtain rendered preview HTML, original URLs, and query strings from private conversations and other restricted content.	6.1	More Details
CVE-2026-77818	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Yordam Information Technology Consulting, Training and Electronic Systems Industry and Trade Inc. Library Information and Document Automation Program allows Content Spoofing. This issue affects Library Information and Document Automation Program: from v22.1 before v22.2.	6.1	More Details
CVE-2026-19727	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Yordam Information Technology Consulting, Training and Electronic Systems Industry and Trade Inc. Library Information and Document Automation Program allows XSS Targeting HTML Attributes. This issue affects Library Information and Document Automation Program: before v22.2.	6.1	More Details
CVE-2026-76755	Vulnerability in Drupal Gammu SMS Daemon. This issue affects Gammu SMS Daemon versions: *.*.	5.9	More Details
CVE-2026-76758	Vulnerability in Drupal Link content parser. This issue affects Link content parser versions: *.*.	5.9	More Details
CVE-2026-86506	In JetBrains GoLand before 2026.2.2.1 missing authentication on the GoLand profiler's injected pprof server exposed profiling data	5.9	More Details
CVE-2026-80125	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	5.9	More Details
CVE-2026-76756	Vulnerability in Drupal Gammu SMS Daemon. This issue affects Gammu SMS Daemon versions: *.*.	5.9	More Details
CVE-2026-86253	h3 (npm package) versions <= 2.0.1-rc.14 contain a path traversal vulnerability in serveStatic(). On Node.js deployments, event.url.pathname is not normalized, so percent-encoded dot segments (%2e%2e) are passed to decodeURI() and decoded to ../ sequences without sanitization. An unauthenticated remote attacker can send crafted requests to endpoints served by serveStatic() to read arbitrary files outside the intended static	5.9	More Details

	directory. Fixed in 1.15.6 and 2.0.1-rc.15.		
CVE-2026-86096	PX4 Autopilot through 1.17.0 contains a use-after-free vulnerability in TemperatureCalibration::start() due to a race condition between task spawning and object deletion. Attackers can trigger the calibration process via shell commands to write to freed heap memory, corrupting unrelated objects or allocator metadata and destabilizing heap operations.	5.9	More Details
CVE-2026-86187	WWBN AVideo generates passwords for external-login accounts using rand() instead of a cryptographic generator, producing only 31-bit integers. Attackers with access to password hashes can recover plaintext passwords in minutes through offline brute-force attacks due to unsalted MD5-based hashing.	5.9	More Details
CVE-2026-84964	A double free in the OpenSSL-based TLS certificate revocation checking path of the MongoDB C Driver can be reached by a TLS endpoint that the client already trusts. During the handshake, specially formed certificate data can cause the same heap object to be released twice. An unauthenticated party acting as the trusted endpoint may cause the connecting client application to terminate unexpectedly.	5.9	More Details
CVE-2026-17539	RTU500 has a vulnerability, where high-load scenarios, such as sending GI requests at short intervals, may cause a NULL pointer dereference in the last entry of the enhanced message queue. This can cause a BCI_IEC104 fatal write error, resulting in connection interruption and restart, and ultimately a denial of service for bidirectional IEC 60870-5-104 communication.	5.9	More Details
CVE-2026-80438	The Ninja Forms WordPress plugin before 3.15.2 does not restrict its REST abilities to administrators, accepting a Ninja Forms WordPress plugin before 3.15.2-specific capability as equivalent to full site administration, which allows any user granted that capability to read Ninja Forms WordPress plugin before 3.15.2 settings and stored form submissions, overwrite the Ninja Forms WordPress plugin before 3.15.2's configuration, and create or modify arbitrary posts and pages. The capability belongs to no default WordPress role and the Ninja Forms WordPress plugin before 3.15.2 never grants it, so an administrator must have assigned it, typically when delegating access to the form builder.	5.9	More Details
CVE-2024-3773	The LiveJournal Shortcode WordPress plugin through 1.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.9	More Details
CVE-2026-81347	The Frontend Admin by DynamiApps WordPress plugin before 3.29.13 does not properly validate a user-controllable directory path before deleting files within it, allowing unauthenticated attackers to delete index.php and .htaccess files outside the intended directory, including the WordPress root, which can render the site inoperable. Successful exploitation requires a non-default form configuration.	5.9	More Details
CVE-2026-86251	h3 versions before 1.15.9 contain a path traversal vulnerability in the serveStatic utility. A double-decoding flaw allows a request path containing double-encoded dot sequences (e.g. %252e%252e) to be decoded to %2e%2e, which survives resolveDotSegments() because that function only checks for literal '.' characters. When the resulting asset ID is resolved by URL-based backends (CDN, S3, object storage), %2e%2e is interpreted as '..' per RFC 3986, enabling path traversal to read arbitrary files from the backend.	5.9	More Details
CVE-2026-86258	nbviewer through 1.0.1 contains a path traversal vulnerability in LocalFileHandler.can_show() that uses string-prefix comparison instead of proper path validation. Attackers can read files from sibling directories outside the configured root by requesting paths that share the root as a textual prefix, disclosing unintended notebooks and credentials.	5.9	More Details
CVE-2026-84378	HTTPX2 is a next generation HTTP client for Python. From 2.5.0 until 2.10.0, the HTTPX2 Server-Sent Events parser in src/httpx2/httpx2/_sse.py repeatedly copies and rescans buffered text in _SSELineDecoder.decode() when an attacker-controlled or compromised SSE endpoint splits one unterminated line across many response chunks. The behavior affects httpx2.Client.sse() and httpx2.AsyncClient.sse(), and the total processing work grows quadratically with the line length, allowing a crafted stream to consume excessive CPU and block a synchronous worker or asynchronous event loop. This issue is fixed in version 2.10.0.	5.9	More Details
CVE-2026-84890	undici's decompress interceptor decompresses response bodies according to the untrusted Content-Encoding header. While the number of content-encoding layers is capped, the total decompressed output size is unbounded and there is no configuration option to limit it. A malicious or faulty upstream can therefore return a small compressed payload, a compression bomb, that expands to hundreds of megabytes or more in client memory, an asymmetric resource consumption that can exhaust memory and crash the process. This affects undici versions from 7.15.0 up to 7.29.1 and from 8.0.0 up to 8.10.2. Users should upgrade to undici 7.29.1 or 8.10.2.	5.9	More Details
CVE-2026-79734	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	5.9	More Details
CVE-2026-73310	XenForo before 2.3.13 contains an authorization flaw in the OAuth2 token endpoint that allows attackers controlling any allowlisted redirect URI to bypass redirect URI binding by submitting a different allowlisted URI than the one recorded at authorization time. Attackers can exchange an intercepted authorization code using a mismatched redirect URI to steal OAuth2 tokens from intercepted authorization flows.	5.9	More Details

CVE-2026-20354	Multiple vulnerabilities in the Secure/Multipurpose Internet Mail Extensions (S/MIME) decryption functionality of Cisco Secure Email could allow an unauthenticated, remote attacker to recover plain text from encrypted email messages. These vulnerabilities are due to insufficient validation of message integrity. An attacker could exploit these vulnerabilities by using a machine-in-the-middle technique to intercept and modify traffic between email gateways. A successful exploit could allow the attacker to obtain plaintext content from the encrypted communication.	5.9	More Details
CVE-2026-20355	Multiple vulnerabilities in the Secure/Multipurpose Internet Mail Extensions (S/MIME) decryption functionality of Cisco Secure Email could allow an unauthenticated, remote attacker to recover plain text from encrypted email messages. These vulnerabilities are due to insufficient validation of message integrity. An attacker could exploit these vulnerabilities by using a machine-in-the-middle technique to intercept and modify traffic between email gateways. A successful exploit could allow the attacker to obtain plaintext content from the encrypted communication.	5.9	More Details
CVE-2026-61614	SolidInvoice is an open-source invoicing platform. Prior to version 3.0.1, the REST API authenticator accepts bearer tokens via a `?token=` URL query parameter as a fallback to the `X-API-TOKEN` header. This causes long-lived API credentials to be recorded in server access logs, proxy logs, browser history, and HTTP Referer headers sent to third-party origins. Version 3.0.1 fixes the issue.	5.9	More Details
CVE-2026-76757	Vulnerability in Drupal Gammu SMS Daemon. This issue affects Gammu SMS Daemon versions: *.*.	5.9	More Details
CVE-2026-85024	undici bundles a WebSocket client whose permessage-deflate size-limit cleanup removes all listeners from the internal zlib inflate stream, including its error listener, while that stream can still emit. When a remote peer sends a compressed payload that crosses the built-in 128 MiB decompressed-payload limit and then contains a malformed DEFLATE byte, the inflate stream emits a data error with no listener attached, which Node.js treats as a fatal unhandled error and terminates the entire process. Exploitation is remote and unauthenticated, requires no application mistake, and is asymmetric, since roughly 130 KB on the wire expands past the limit and crashes the process, and reconnecting can repeat the crash. This affects undici versions from 6.25.0 up to 6.28.1, from 7.28.0 up to 7.29.1, and from 8.1.0 up to 8.10.2. Users should upgrade to undici 6.28.1, 7.29.1, or 8.10.2.	5.9	More Details
CVE-2026-84766	Unauthenticated Bypass Vulnerability in FluentBooking Pro <= 2.2.1 versions.	5.9	More Details
CVE-2026-85534	A flaw was found in libsoup. When a client sends an HTTP/2 request body from a non-pollable input stream, the library can buffer more data than the current flow-control window later allows. A malicious HTTP/2 server can shrink SETTINGS_INITIAL_WINDOW_SIZE while that buffered read is still in progress. The client then copies the full buffer into a smaller DATA callback without a runtime bounds check, which can abort the process or fail the HTTP/2 session.	5.9	More Details
CVE-2026-9036	IBM Netezza Software 11.3.0.3 through Interim Fix 002 does not validate or improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2026-85014	undici's experimental WebSocketStream client crashes the whole Node.js process when a remote peer closes the TCP connection without a WebSocket close handshake. On an unclean close the internal socket-close handler calls abort on the writable stream unconditionally and discards the returned promise, but per the WHATWG Streams standard aborting a locked writable returns a promise that rejects with a TypeError. Because the application holds a writer on that writable, which is the only way to write, the rejection is never observed and Node's default unhandled-rejection behavior terminates the process. An untrusted server can therefore crash a client with a single abrupt disconnect, with no authentication and no application mistake. This affects undici versions from 7.0.0 up to 7.29.1 and from 8.0.0 up to 8.10.2. Users should upgrade to undici 7.29.1 or 8.10.2.	5.9	More Details
CVE-2026-3416	The API Publisher component previously used a non-cryptographic pseudorandom number generator (PRNG) to create shared secrets for Webhook HMAC validation. This PRNG lacks sufficient entropy for security-sensitive operations, allowing a sophisticated attacker to predict future secrets. This enables malicious actors to forge event payloads with valid HMAC signatures, bypassing the API Gateway's authenticity verification. Successful exploitation could allow an attacker to predict shared secrets used for Webhook HMAC validation and forge event payloads with valid signatures. This may enable bypassing API Gateway authenticity checks, leading to unauthorized event injection, data manipulation, or downstream system compromise.	5.9	More Details
CVE-2026-84185	A flaw was found in the jwcrypto library, which is used for implementing Javascript Object Signing and Encryption (JOSE) standards. The issue occurs when the library verifies a General JSON Serialization JWS using a set of keys. Due to a coding error, the library fails to correctly identify the specific key ID (kid) and may instead accept a signature made by any valid key in the set. This can allow an attacker with a valid key to bypass authorization checks in applications that rely on the key ID to identify specific tenants or users.	5.9	More Details
	undici's retry handler can leave an already-exposed response body pending forever. When a server returns a		

CVE-2026-18149	successful response that declares a Content-Length, sends only part of the body, and closes the connection, the retry handler retries the request. If the retry returns a non-retryable status such as 400, the handler forwards that new response downstream and replaces its internal response stream, but the original response body that the application still holds is never ended or destroyed. As a result calls that read that body never settle, and the configured body timeout does not fire because its timer is tied to the connection parser rather than the orphaned body. An attacker-controlled server can trigger this with two short responses without keeping a connection open, and repeated requests accumulate pending promises and streams that can exhaust application concurrency or memory. This affects undici versions from 7.11.0 up to 7.29.1 and from 8.0.0 up to 8.10.2. Users should upgrade to undici 7.29.1 or 8.10.2.	5.9	More Details
CVE-2026-76925	A flaw was found in Flatpak. A Time-of-check to time-of-use (TOCTOU) race condition exists in the `org.freedesktop.Flatpak.SystemHelper` component. This vulnerability occurs because a privileged `chmod` operation executes before the OSTree repository validation within the `Deploy()` function. An attacker can exploit this timing window to redirect symlinks to arbitrary files, potentially leading to unauthorized file manipulation or information disclosure.	5.8	More Details
CVE-2026-84815	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kriesi Enfold allows Reflected XSS. This issue affects Enfold: from n/a through 8.0.	5.8	More Details
CVE-2026-77698	Zohocorp ManageEngine Endpoint Central versions before 11.5.2605.01 are vulnerable to local privilege escalation due to Agent upgrade.	5.7	More Details
CVE-2026-16180	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 Toolkit could allow an authenticated user to cause a denial-of-service condition due to improper validation of XML entities.	5.7	More Details
CVE-2026-79642	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	5.6	More Details
CVE-2026-86144	In xinclude in libxml2 before 2.15.4, xmlXIncludeProcess and xmlXIncludeProcessTree do not propagate parseFlags. This has security relevance for, for example, the XML_PARSE_NONET flag, if (without it) a custom resource loader accesses the internet and triggers XML external entity injection, SSRF, or a denial of service (e.g., for an attacker-controlled internet resource that is intentionally slow).	5.6	More Details
CVE-2026-84380	HTTPX2 is a next generation HTTP client for Python. Prior to 2.11.0, Request._prepare() in src/httpx2/httpx2/_models.py can add a body-derived Content-Length header to a request that already contains a caller-supplied Transfer-Encoding header because its setdefault() processing checks each default header independently rather than treating the two framing headers as mutually exclusive. Fixed-size byte, JSON, form, and known-length multipart bodies can therefore be serialized over HTTP/1.1 with both headers, allowing request smuggling or connection desynchronization when downstream intermediaries disagree about which framing header takes precedence. This issue is fixed in version 2.11.0.	5.6	More Details
CVE-2026-85639	A security vulnerability has been detected in jofpin trape 2.0. This vulnerability affects unknown code of the file core/user.py of the component Telemetry Endpoint. Such manipulation of the argument vId leads to race condition. The attack can be executed remotely. Attacks of this nature are highly complex. It is stated that the exploitability is difficult. 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.	5.6	More Details
CVE-2026-49831	DSpace open source software is a repository application which provides durable access to digital resources. Prior to versions 7.6.7, 8.4, 9.3, and 10.0, the Curation Task feature allows an output path to be used by the reporter (-r parameter), typically used to stream results and status of curation task operations. It is not restricted to any particular base path, meaning that any path writable by the DSpace (often 'tomcat') user is allowed. This constitutes a Path Traversal Vulnerability in the curate script. This issue has been patched in versions 7.6.7, 8.4, 9.3, and 10.0.	5.5	More Details
CVE-2026-6244	libpcap BPF interpreter for the 'div #k' and 'mod #k' ALU instructions does not check whether the immediate value is zero. In particular uncommon use cases a crafted filter program can cause a division by zero.	5.5	More Details
CVE-2026-85698	Turso through 0.8.0-pre.8 contains an out-of-bounds read vulnerability in the table-leaf page reader that uses an attacker-controlled cell-count field without bounds validation. Attackers can craft a malicious database file with a modified cell count value to trigger an index-out-of-bounds panic when querying, causing denial of service in any application that opens untrusted database files.	5.5	More Details
CVE-2026-82194	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.134 does not validate a user supplied path before using it in a file deletion routine, allowing administrators to delete arbitrary files on the server, including files outside the web root.	5.5	More Details
CVE-	CDT before 1.4.5 contains an out-of-bounds read vulnerability in the opposedVertexInd() function when constraint edge intersections are computed in floating point and round outside adjacent triangles. Attackers		More

2025-15647	can supply nearly-degenerate constraint edges through geometry data to trigger an out-of-bounds array access that crashes the calling process.	5.5	Details
CVE-2026-82193	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.134 does not validate a user supplied file name before using it to build a write path, allowing administrators to write files of permitted types to arbitrary locations on the server and to overwrite existing files.	5.5	More Details
CVE-2026-31911	libpcap BPF interpreter calls abort() if it encounters a BPF instruction that has an invalid opcode. In particular uncommon use cases a crafted filter program can terminate the OS process.	5.5	More Details
CVE-2026-20516	In MiracastService, there is a possible escalation of privilege due to a confused deputy. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11060069 / DTV04881615; Issue ID: MSV-7882.	5.5	More Details
CVE-2026-79975	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Certificate Validation vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to server-side request forgery.	5.5	More Details
CVE-2026-86500	In JetBrains YouTrack before 2026.1.14047 a missing escalation check let a user with project update permissions grant themselves Project Admin	5.5	More Details
CVE-2026-80167	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Use of Hard-coded Cryptographic Key vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure.	5.5	More Details
CVE-2026-82062	A security issue in MongoDB Server allows an authenticated user with elevated internal privileges to bypass a disabled feature gate in the applyOps command by specifying an internal replication mode value that was not intended to be client-selectable. This bypass enables execution of container operations that are disabled by default in production configurations, allowing direct storage-engine writes to arbitrary internal storage tables. The authorization check for these operations validates only the operation's namespace, not the actual storage target, enabling writes to unrelated internal metadata or other collections' data.	5.5	More Details
CVE-2026-85456	MOOS-IvP through 24.8.1 fails to properly validate variable names extracted from alog files in the SplitHandler, allowing attackers to write files outside the split directory. Attackers can supply crafted alog files with backslash sequences in variable names to escape the output directory and append to arbitrary files on Windows systems.	5.5	More Details
CVE-2026-82918	XG VisionTerminal and XG-X VisionTerminal provided by Keyence Corporation improperly restrict XML external entity references. If a user opens a specially crafted setting file, the sensitive information stored in the system where XG VisionTerminal or XG-X VisionTerminal is installed may be disclosed.	5.5	More Details
CVE-2026-20515	In gpu, there is a possible system crash due to use after free. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS11122991; Issue ID: MSV-8132.	5.5	More Details
CVE-2026-49833	DSpace open source software is a repository application which provides durable access to digital resources. From versions 8.0-rc1 to before 8.4, 9.0-rc1 to before 9.3, and 10-rc1 to before 10.0, a path traversal vulnerability is possible via the COAR Notify / LDN service in DSpace. The attacker MUST already have DSpace administrator credentials in order to perform the attack. When reading a file input stream of an "inbound pattern" / "template", used to generate an LDN message, the LDN class does not check for path traversal or restrict the templates to a known base path. This could allow an untrusted file from elsewhere in the file system (e.g. an export log, a bitstream path, a temporary file) to be read and interpreted as an Apache Velocity template. This issue has been patched in versions 8.4, 9.3, and 10.0.	5.5	More Details
CVE-2026-31912	libpcap BPF interpreter detects neither reaching the end of the filter program buffer due to lack of a return instruction nor executing a jump instruction with an offset that translates to a pointer outside of the buffer. In particular uncommon use cases a crafted filter program can cause the interpreter to try reading the OS process memory in the 32GiB around the buffer on 64-bit architectures and in the entire address space on 32-bit architectures.	5.5	More Details
CVE-2026-80054	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.	5.5	More Details
CVE-2026-80057	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Use of Hard-coded Cryptographic Key vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure.	5.5	More Details
CVE-2026-	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local	5.5	More Details

80056	access could potentially exploit this vulnerability, leading to information exposure.		
CVE-2026-14255	A maliciously crafted IFC file, when parsed through certain Autodesk products, can trigger an Uncontrolled Recursion vulnerability. A malicious actor may leverage this vulnerability to cause the application to terminate unexpectedly, resulting in a denial-of-service. Exploitation requires a user to open a specially crafted IFC file.	5.5	More Details
CVE-2026-17440	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a local attacker to cause a denial of service due to uncontrolled recursion.	5.5	More Details
CVE-2026-80178	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	5.5	More Details
CVE-2026-80058	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Cleartext Storage of Sensitive Information vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	5.5	More Details
CVE-2026-6554	libpcap BPF interpreter treats the offset in the 'ja L' BPF instruction as a signed integer to implement looping via backward jumps, but it does not limit the number of loop iterations. In particular uncommon use cases a crafted filter program can cause the interpreter to loop infinitely.	5.5	More Details
CVE-2026-84772	Editor Server Side Request Forgery (SSRF) in Broken Link Checker <= 2.4.14 versions.	5.5	More Details
CVE-2026-78487	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Use of Hard-coded Cryptographic Key vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure.	5.5	More Details
CVE-2026-20500	In Modem, there is a possible system crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is needed for exploitation. Patch ID: MOLY01810811; Issue ID: MSV-9232.	5.5	More Details
CVE-2026-52772	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, Bazar form-field templates still apply |raw('html') to field.label / field.hint in attribute and label-body contexts, resulting stored XSS in form renders. This issue has been patched in version 4.6.6.	5.5	More Details
CVE-2026-82525	Exterro FTK Imager before 8.3 contains an XML external entity (XXE) injection vulnerability that allows attackers to read arbitrary files from the host filesystem by embedding malicious external entity references and attacker-controlled XSLT stylesheets within a Report.xml file inside a UFDR ZIP evidence item. Attackers can craft a malicious UFDR archive that, when previewed by an examiner, causes the XML parser to resolve file:// external entity references and execute msxsl:script within the external stylesheet to exfiltrate the resolved file contents to an attacker-controlled endpoint via a generated image URL.	5.5	More Details
CVE-2026-78601	Missing Authorization (CWE-862) in Kibana can lead to information disclosure via Privilege Abuse (CAPEC-122). An authorization control was not applied to a Kibana Entity Store configuration operation, allowing an authenticated user with elevated Kibana privileges to indirectly cause a background task to read from Elasticsearch indices that user is not authorized to access. Derived entity data from those indices is then exposed through the entity store output.	5.5	More Details
CVE-2026-66652	Cross-Site Request Forgery (CSRF) vulnerability in ThemeGoods Grand Tour allows Cross Site Request Forgery. This issue affects Grand Tour: from n/a through 5.5.1.	5.4	More Details
CVE-2026-15247	The Search Atlas SEO WordPress plugin before 2.6.24 does not perform a nonce or capability check before processing a settings update in one of its early-priority handlers, allowing any authenticated user such as a Subscriber to overwrite or delete the site's stored Google service-account credentials.	5.4	More Details
CVE-2026-33391	An access control vulnerability was discovered in the Smart Polling configuration functionality due to insufficient validation of user privileges. An authenticated user with limited privileges can remotely bypass the intended access control of the web management interface and modify the Smart Polling discovery configuration. This allows the attacker to disrupt the visibility of assets in the monitored network.	5.4	More Details
CVE-2026-86714	PX4 Autopilot through 1.17.0 contains a stack buffer over-read vulnerability in the netman system command that fails to validate interface name length. Attackers can supply interface names of 74 bytes or more via the -i option to read beyond buffer boundaries, leaking stack memory to console output or writing it into persistent network configuration files.	5.4	More Details
CVE-2026-85593	phpMyFAQ versions before 4.1.8 contain a stored cross-site scripting vulnerability in FaqHelper::convertOldInternalLinks() that calls html_entity_decode() on sanitized FAQ content, reversing entity-encoding protection. Authenticated users with FAQ editing privileges can inject JavaScript payloads	5.4	More Details

	that execute in the browsers of all users viewing the affected FAQ pages.		
CVE-2026-84664	Jenkins GitLab Plugin 1.9.16 and earlier allows overwriting the global GitLab connection configuration through Stapler data binding, allowing attackers to connect to an attacker-specified URL using GitLab API tokens already configured by administrators.	5.4	More Details
CVE-2026-78598	Incorrect Authorization (CWE-863) in the Kibana machine learning feature can lead to information disclosure via Exploiting Incorrectly Configured Access Control Security Levels (CAPEC-180). An authenticated user holding machine learning job management privileges within a single Kibana space could cause a job's saved object to become accessible across all spaces in the Kibana instance, without holding access rights to those additional spaces.	5.4	More Details
CVE-2026-84701	NocoBase fails to sanitize rich text field values in the read renderer, allowing users with create permissions to store malicious HTML with event handlers. Attackers can write arbitrary markup through the collection API that executes in the browsers of all users viewing the affected record.	5.4	More Details
CVE-2026-81164	Missing Authorization vulnerability in Drupal Entity PDF allows Forceful Browsing. This issue affects Entity PDF versions: from 0.0.0 to 2.1.5.	5.4	More Details
CVE-2026-82024	LearnPress WordPress Plugin before 4.4.6 contains a stored cross-site scripting vulnerability that allows authenticated attackers with the Instructor role to inject persistent malicious payloads by submitting unsanitized input into quiz question answer title fields. Attackers can store arbitrary JavaScript through the answer title parameter, which is rendered through an unescaped HTML sink to execute in the browsers of any user who views the affected quiz question, including students, other instructors, and administrators.	5.4	More Details
CVE-2026-85650	Trigger.dev before 4.5.2 contains a server-side request forgery vulnerability in webhook alert channel delivery URLs that are fetched without validation or SSRF protection. Authenticated users with organization membership can create alert channels with URLs targeting internal services and metadata endpoints, allowing the server to issue POST requests to restricted resources.	5.4	More Details
CVE-2026-85158	AVideo through commit c91b5975d contains a reflected cross-site scripting vulnerability in videoEmbeded.php that echoes the link parameter inside an HTML comment with zero escaping. Attackers can close the comment with --> and inject arbitrary JavaScript that executes when victims visit the crafted embed URL.	5.4	More Details
CVE-2026-19057	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Gastromenum Gastromenum Ticket and QR Menu System allows Stored XSS. This issue affects Gastromenum Ticket and QR Menu System: before 2026.08.31.	5.4	More Details
CVE-2026-17274	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to predictable server seeds.	5.4	More Details
CVE-2026-16892	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to improper authentication during service-name matching.	5.4	More Details
CVE-2026-12843	The LearnDash LMS plugin for WordPress is vulnerable to authorization bypass in versions 4.25.0 - 5.1.6. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to enroll arbitrary users in paid courses without payment verification, bypassing the entire payment system and gaining unauthorized access to premium educational content.	5.4	More Details
CVE-2026-86719	WWBN AVideo through commit c3edcc274c389816d434acadac07ee78eaf330c1 (master) contains a cross-site request forgery vulnerability in the CustomizeUser plugin endpoint plugin/CustomizeUser/swapUser.json.php. The endpoint takes users_id from $_REQUEST and invokes User::swapUser() without calling forbidIfNotPost() or forbidIfInvalidToken(), and the global autoCSRFGuard() check only runs for POST requests to *.json.php, so the action is reachable via GET. An attacker who causes an authenticated administrator's browser to issue a cross-origin GET (for example via an <img> tag or link) can replace that administrator's session with a non-admin user account, causing the administrator to lose administrative access until the swap is cancelled; swapping to another administrator account is rejected, so this is not privilege escalation. The JSON response also discloses the session_id. The CustomizeUser plugin is enabled by default, and no patch was available at the time of publication.	5.4	More Details
CVE-2026-84666	Jenkins Job Configuration History Plugin 1367.vc8fa_b_15101dc and earlier allows overwriting the plugin's history recording configuration through Stapler data binding, allowing attackers to redirect history storage to an attacker-specified directory and modify history recording settings.	5.4	More Details
CVE-2026-81583	The My Login WordPress plugin before 7.2.0 does not enforce the network's registration setting when processing site signups on multisite installations, allowing users with a subscriber account, and unauthenticated users on some networks, to create new sites and be granted administrator over them.	5.4	More Details
CVE-			

2026-84330	UI misrepresentation in FullScreen in Google Chrome on on Android prior to 152.0.7977.75 allowed a remote attacker to spoof address bar via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2026-85541	DreamMaker developed by Interinfo has a Reflected Cross-site Scripting vulnerability. Authenticated remote attackers can execute arbitrary JavaScript codes in user's browser via a malicious website.	5.4	More Details
CVE-2026-2811	The Ajaxify Comments WordPress plugin before 3.2 is vulnerable to HTTP Header Injection due to insufficient input sanitization and output escaping on user-supplied data. This makes it possible for unauthenticated attackers to inject arbitrary HTTP headers.	5.4	More Details
CVE-2026-56128	pfSense Plus before 26.07 and CE before 2.9.0 allow authenticated users with the Firewall: Schedules: Edit privilege to inject arbitrary JavaScript via the descr parameter in /firewall_schedule_edit.php. The schedule description is stored without HTML sanitization and subsequently inserted into an HTML attribute value in /firewall_rules.php with only single-quote escaping applied, permitting double-quote breakout. The payload executes in the browser of any user with the Firewall: Rules privilege who views the rules list with the affected schedule attached.	5.4	More Details
CVE-2026-84674	Missing permission checks in Jenkins XebiaLabs XL Deploy Plugin 26.1.0 and earlier allow attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	5.4	More Details
CVE-2026-85601	Grav Admin before 2.0.20 fails to sanitize output from marked.parse() before injecting it into the DOM via Svelte's {@html} directive in MarkdownEditor and MarkdownModal components. Attackers can inject javascript: URI schemes in plugin or theme changelogs to execute arbitrary code in authenticated admin sessions without requiring site access.	5.4	More Details
CVE-2026-85600	Grav Admin (getgrav/grav-plugin-admin2) versions <= 2.0.19 contain a stored cross-site scripting vulnerability in the tHtml() function (src/lib/stores/i18n.svelte.ts), which substitutes untrusted parameters such as usernames into translation templates before parsing the result as markdown. Grav's server-side username validation (DataUser::isValidUsername) blocks filesystem-dangerous characters but not <, >, ", or ', allowing an attacker to register a username containing an HTML payload. When an administrator views a UI surface that renders the username through tHtml()—such as the two-factor force-disable confirmation prompt or the 'page is locked' editor notice—the payload executes in their authenticated session. Fixed in 2.0.21.	5.4	More Details
CVE-2026-84217	Missing Authorization vulnerability in Mamunur Rashid Classified Listing allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Classified Listing: from n/a through 6.1.1.	5.4	More Details
CVE-2026-86436	Lara Dashboard before 1.3.2 fails to authorize access to the post-builder image and video upload endpoints, allowing authenticated accounts without content permissions to upload files. Attackers can upload polyglot files with attacker-chosen extensions to the public web root and execute code if the deployment permits execution of the uploaded file type.	5.4	More Details
CVE-2026-17621	IBM Langflow OSS 1.0.0 through 1.10.2 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot " sequences (/.. /) to view arbitrary files on the system.	5.4	More Details
CVE-2026-2520	The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'updateAddon' function in all versions up to, and including, 27.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update any plugin with a main file of 'main.php' to its latest version.	5.4	More Details
CVE-2026-86416	ILIAS versions before 9.23, 10.11, and 11.4 contain an authorization bypass vulnerability in ilObjGroupGUI where saveMapSettingsObject() and updateGroupTypeObject() perform state-changing operations without write permission checks. Authenticated users with only read access to a group can craft POST requests to modify group map settings and didactic template assignments, changing group modes and permissions for all members.	5.4	More Details
CVE-2026-85159	AVideo through commit c91b5975d contains a reflected cross-site scripting vulnerability in userLogin.php where the cancelUri parameter is echoed in an href attribute after isSafeRedirectURL checks protocol only, not HTML characters. Unauthenticated attackers can inject event handlers via relative URLs with embedded quotes to execute arbitrary JavaScript when users interact with the Cancel button.	5.4	More Details
CVE-2026-56126	pfSense Plus before 26.07 and CE before 2.9.0 allow authenticated users with the Status: Monitoring privilege to inject arbitrary JavaScript via graph configuration parameters in /status_monitoring.php. Multiple POST parameters including graph-left, graph-right, time-period, resolution, start-date, end-date, start-time, end-time, graph-type, invert, and refresh-interval are concatenated and written to the global pfSense XML configuration without sanitization, then echoed unsanitized into a JavaScript string context on page render. Because the setting is stored in the global configuration, the payload executes in the browser of every user who visits the Status: Monitoring page.	5.4	More Details
	The Simple Membership MailChimp Integration WordPress plugin before 1.9.8 does not have CSRF checks in		

CVE-2026-8151	its settings page, allowing attackers to trick a logged-in administrator into changing the configured third-party API key. Once replaced, all subsequent member registration data (name, email, membership level) is sent to the attacker-controlled account.	5.4	More Details
CVE-2026-27432	Authorization Bypass Through User-Controlled Key vulnerability in sc Internet Vivoo WP Rentals allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Rentals: from n/a before 3.16.0.	5.4	More Details
CVE-2026-56127	pfSense Plus before 26.07 and CE before 2.9.0 allow authenticated users with the Firewall: Rules: Edit privilege to inject arbitrary JavaScript via the descr parameter in /firewall_rules_edit.php. The firewall rule description is stored in the pfSense XML configuration with only backslash-escaping applied and no HTML sanitization, then rendered without encoding in the firewall log table in /status_logs_filter.php. The payload executes in the browser of any user with the Status: Logs: Firewall privilege who views the affected log entries.	5.4	More Details
CVE-2026-85577	AVideo through commit c91b5975d contains a reflected cross-site scripting vulnerability in userLogin.php that allows unauthenticated attackers to inject arbitrary JavaScript by closing the script tag with </script>. Attackers can craft a malicious URL with an error parameter containing script breakout sequences to execute arbitrary JavaScript in the victim's browser context on the login page.	5.4	More Details
CVE-2026-18957	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Menulux Software Inc. Menulux Portal allows Stored XSS. This issue affects Menulux Portal: before 20260903211448.	5.4	More Details
CVE-2026-84660	A missing permission check in Jenkins Pipeline: Build Step Plugin 599.v4b_67ea_11b_152 and earlier causes downstream builds triggered by the `build` step to be canceled even when the build's authentication lacks Item/Cancel permission on the downstream job.	5.4	More Details
CVE-2026-12853	The Flamingo plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.6.2. 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 enumerate taxonomy terms including channel names derived from Contact Form 7 form titles that may reveal internal form purposes, department names, or workflow identifiers, as well as submission counts per channel and contact tag names. The plugin's flamingo_map_meta_cap() filter restricts access to Flamingo's admin UI but does not extend to WordPress core APIs such as XML-RPC wp.getTerms and admin-ajax ajax-tag-search.	5.4	More Details
CVE-2026-84806	Kimai before 2.63.0 contains an improper authorization vulnerability in team access endpoints that allows authenticated users with team edit permissions and read-only access to grant team access to customers, projects, or activities. Attackers can exploit insufficient permission checks by sending POST requests to team access endpoints to modify access control lists for entities they should not be able to modify.	5.4	More Details
CVE-2026-84661	A missing permission check in Jenkins Pipeline: Build Step Plugin 599.v4b_67ea_11b_152 and earlier causes downstream builds awaited by the `waitForBuild` step when the `propagateAbort` parameter is used to be canceled even when the build's authentication lacks Item/Cancel permission on the downstream job.	5.4	More Details
CVE-2026-86257	wger before 2.6 fails to sanitize first_name and last_name fields in the gym member TSV export endpoint, allowing any gym member to inject spreadsheet formulas. Attackers can inject formulas like =HYPERLINK to exfiltrate admin data or execute code when admins open the exported file in Excel or LibreOffice Calc.	5.4	More Details
CVE-2026-86256	wger before 2.6 (affected versions <= 2.5.0) contains an open redirect vulnerability in the trainer_login view (wger/core/views/user.py). After a trainer enters impersonation mode, the view redirects to the user-supplied 'next' GET parameter via HttpResponseRedirect() without validating it with url_has_allowed_host_and_scheme(). An attacker who delivers a crafted link to an authenticated trainer can redirect the trainer's browser to an attacker-controlled domain, enabling phishing and leaking the wger URL structure (including the impersonated user's user_pk) via the Referer header.	5.4	More Details
CVE-2026-84385	A improper access control vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.6, FortiSOAR PaaS 7.5.0 through 7.5.3, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.6, FortiSOAR on-premise 7.5.0 through 7.5.3, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow attacker to escalation of privilege via <insert attack vector here>	5.4	More Details
CVE-2026-84804	Kimai before 2.65.0 fails to properly validate permissions when removing team access to activities, projects, and customers via API endpoints. Authenticated users with edit_team permission can revoke team access without the required permissions_activity check, bypassing authorization controls.	5.4	More Details
CVE-2026-84677	Jenkins update-center2 3.18.3 and earlier does not escape plugin-provided values (plugin names, descriptions, and version metadata) on plugin download index pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a plugin for hosting.	5.4	More Details
CVE-2026-	libjxl before 0.12 contains an integer underflow vulnerability in the container box parser that allows remote attackers to inject arbitrary metadata by exploiting 64-bit box size truncation to size_t on 32-bit platforms. Attackers can supply a crafted JPEG XL file causing the decoder to parse attacker-controlled codestream	5.4	More

82522	bytes as phantom box headers, enabling injection of arbitrary metadata (Exif, XMP, IPTC, JUMBF) and potential out-of-bounds reads.		Details
CVE-2026-79418	EMX Tecnologia Gestao X version <= 8.4 contains a Stored Cross-Site Scripting (XSS) vulnerability in the Help Chat functionality. Improper neutralization of user-controlled input during web page generation allows authenticated attackers to execute arbitrary JavaScript in the context of other authenticated users, potentially resulting in session hijacking, account takeover, and unauthorized actions.	5.4	More Details
CVE-2026-73476	Improper Handling of Case Sensitivity vulnerability in Drupal External Authentication allows Privilege Escalation. This issue affects External Authentication versions: from 0.0.0 to 2.0.13.	5.4	More Details
CVE-2026-85177	CRMEB through 6.0.0 fails to validate message ownership in the edit_message handler of MessageSystemController.php, allowing authenticated users to modify arbitrary system inbox messages. Attackers can update any message's columns including is_del, look, and uid to delete, mark read, or reassign victim notifications without authorization.	5.4	More Details
CVE-2026-85305	Server-Side Request Forgery (SSRF) vulnerability in SEOPress allows Server Side Request Forgery. This issue affects SEOPress: from n/a through 10.1.	5.4	More Details
CVE-2026-55513	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. From version 0.3.0 to before version 0.5.0, the nebula-mgmt Web UI host-creation path ignores both the server-wide enrollment_token_ttl security setting and per-network network_config.enrollment_token_ttl overrides. API host creation and token-regeneration paths use the configured TTL resolver, but POST /ui/hosts hardcodes now.Add(24 * time.Hour) for newly minted agent enrollment tokens. In deployments that intentionally reduce enrollment-token lifetime, any authenticated operator who can create a host through the Web UI can still mint a bearer enrollment token valid for about 24 hours. This issue has been patched in version 0.5.0.	5.4	More Details
CVE-2025-14945	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via event attribute values in all versions up to, and including, 7.3.3. This is due to insufficient input sanitization when storing attribute values (using only `wp_unslash()` without sanitization) and lack of output escaping when rendering the '#_ATT{key}' placeholder. This makes it possible for authenticated attackers, with Author-level access and above, or unauthenticated attackers when anonymous event submissions are enabled, to inject arbitrary web scripts that execute when any user views the affected event page.	5.4	More Details
CVE-2026-84807	Kimai (kimai/kimai) through 2.65.0 contains a business logic / improper authorization vulnerability in the default team creation endpoints. An authenticated user with project permission-management privileges can create or use a customer, project, or activity whose name matches an existing team; because the endpoints POST /api/customers/{id}/team, POST /api/projects/{id}/team, and POST /api/activities/{id}/team reuse an existing team of the same name and add the current user as teamlead without verifying that the user is authorized to manage that team, the attacker gains unauthorized team-lead (administration) rights over the existing team. Fixed in 2.65.0.	5.4	More Details
CVE-2026-86205	h3 versions before 2.0.1-rc.18 contain an open redirect vulnerability in the redirectBack() utility that fails to sanitize protocol-relative paths in the Referer header pathname. Attackers can craft a same-origin URL with a double-slash path segment that passes origin validation but produces a Location header interpreted by browsers as a protocol-relative redirect to an external domain.	5.4	More Details
CVE-2026-86178	Pixelfed through 0.12.9 fails to validate follower status in StoryComposeController react and comment endpoints, allowing authenticated users to access follower-only stories. Attackers can enumerate sequential story IDs and submit reactions or comments to retrieve story media URLs and author information without following the account.	5.4	More Details
CVE-2026-84663	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline: Groovy Libraries Plugin 798.v5cc688825312 and earlier allows attackers to delete shared library caches.	5.4	More Details
CVE-2026-86483	In JetBrains YouTrack before 2026.2.18634 stored XSS via a custom field on Agile board cards was possible	5.4	More Details
CVE-2026-78609	Incorrect Authorization (CWE-863) in Elastic Cloud on Kubernetes (ECK) can lead to unauthorized modification of data via Metadata Spoofing (CAPEC-690). An actor holding limited Kubernetes permissions confined to a single namespace could cause attacker-controlled certificate material to be included in the Elasticsearch client trust bundle managed by ECK in a separate namespace.	5.4	More Details
CVE-2026-	In MongoDB, insufficient validation of shard key values during document insertion allowed authenticated users to store documents with specially crafted, operator-shaped objects as shard key values in sharded collections. When change stream events for such documents were processed with the updateLookup full document mode, the crafted values were embedded into internal post-image lookup queries without proper	5.4	More

82060	sanitization, causing them to be interpreted as query operators rather than literal equality values. This could result in change stream consumers receiving incorrect post-image documents or encountering non-resumable fatal errors.		Details
CVE-2026-86112	BookWyrm through 0.9.1 fails to validate user visibility permissions in the Favorite and Unfavorite views, allowing authenticated attackers to favorite or unfavorite followers-only and direct statuses they cannot access. Attackers can POST to the favorite endpoint with a status ID to create unauthorized interactions, trigger ActivityPub broadcasts, and enumerate private status IDs through response differentiation.	5.4	More Details
CVE-2026-84654	In Stapler 2107.v8dfcb_e8ed317 and earlier, except 2088.2093.vd7c3e58008a_6, included in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, form data binding allows setting public static fields of the bound configuration object, allowing attackers who can submit configuration forms to modify public static fields of the configuration objects those forms are bound to, resulting in changes that apply globally to the Jenkins instance.	5.4	More Details
CVE-2026-85090	FreeRDP before 3.31.0 contains a heap out-of-bounds read vulnerability in the general_ChromaV1ToYUV444 function during AVC444 chroma plane reconstruction. A malicious RDP server can craft a RFX_AVC444_BITMAP_STREAM with specific frame geometry to trigger an out-of-bounds memory read past the allocated luma plane.	5.4	More Details
CVE-2026-84835	Missing Authorization vulnerability in DimaFreund Rentsyst allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Rentsyst: from n/a through 2.1.2.	5.3	More Details
CVE-2026-84857	A flaw has been found in sigoden aichat up to 0.30.4. This affects an unknown function of the file src/serve.rs of the component API Endpoint. This manipulation causes uncontrolled memory allocation. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-85381	A security vulnerability has been detected in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. This issue affects some unknown processing of the file App/Home/Controller/ChapterController.class.php of the component Chapter Controller. Such manipulation of the argument content leads to authorization bypass. The attack may be launched remotely. The exploit has been disclosed publicly and may 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.	5.3	More Details
CVE-2026-8279	The Masteriyo LMS plugin for WordPress is vulnerable to unauthorized data deletion due to a missing capability check on the 'delete_item_permissions_check' function in the CourseProgressItemsController in all versions up to, and including, 2.2.0. This makes it possible for unauthenticated attackers to delete arbitrary course progress records belonging to any student.	5.3	More Details
CVE-2026-9736	IBM Netezza Software 11.3.0.3 through Interim Fix 002 could allow an unauthorized user to inject data into log messages due to improper neutralization of special elements when written to log files.	5.3	More Details
CVE-2026-84697	Mailpit's IsInternalIP deny list function fails to block the Azure WireServer address 168.63.129.16 and the RFC 2765/6145 IPv4-translated IPv6 prefix, allowing server-side request forgery to internal destinations. Attackers can supply hostnames resolving to these addresses in message content to reach the link check API and proxy endpoint for accessing internal resources.	5.3	More Details
CVE-2026-84886	A vulnerability was determined in simular-ai Agent-S up to 0.3.2. Affected by this vulnerability is the function ImageData of the file gui_agents/s1/utils/ocr_server.py of the component OCR HTTP API. Executing a manipulation of the argument img_bytes can lead to resource consumption. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-9744	IBM Netezza Software 11.3.0.3 through Interim Fix 002 does not validate or improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle techniques.	5.3	More Details
CVE-2026-85304	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.17.	5.3	More Details
CVE-2026-85309	Missing Authorization vulnerability in Supsystic Ultimate Maps by Supsystic allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ultimate Maps by Supsystic: from n/a through 1.5.3.	5.3	More Details
CVE-	A flaw was found in GLib2. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION and creating the .goutputstream-XXXXXX temporary file fails, the library unlinks the destination and recreates it		More

2026-86469	without exclusive creation or symlink protection. A local attacker who can write to the destination directory can win that race and redirect the write to another file.	5.3	Details
CVE-2026-81205	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in Drupal LDAP / Active Directory Integration allows LDAP Injection. This issue affects LDAP / Active Directory Integration versions: from 0.0.0 to 2.2.1.	5.3	More Details
CVE-2026-85637	A security flaw has been discovered in jofpin trape 1.0.0/2.0. Affected by this issue is the function join_room of the file core/sockets.py of the component Admin Endpoint. The manipulation results in missing authentication. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-86432	commonmark versions from 2.0.0 before 2.8.4 contain a denial of service vulnerability in XmlRenderer that emits depth-proportional indentation for every XML tag. Attackers can provide deeply nested Markdown or AST structures to cause quadratic memory consumption and output amplification, exhausting server resources.	5.3	More Details
CVE-2026-81165	Incorrect Authorization vulnerability in Drupal Blazy allows Forceful Browsing. This issue affects Blazy versions: from 0.0.0 to 3.0.18.	5.3	More Details
CVE-2026-86308	A vulnerability was detected in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. This issue affects some unknown processing of the file App/Common/Conf/config.php of the component Debug Mode. The manipulation of the argument DB_DEBUG results in information disclosure. 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.	5.3	More Details
CVE-2026-55512	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. From version 0.2.0 to before version 0.5.0, when OIDC is enabled, GET /ui/oidc/login is reachable without authentication and is registered outside the Web UI rate-limited auth routes. Every request creates a fresh random OIDC state value and stores it in an in-memory map for 10m. Expired states are swept lazily, but there is no rate limit or maximum live-state cap on the allocation path. An unauthenticated remote client can therefore grow OIDC.states for the full state TTL, bounded by request throughput rather than by configured auth rate limits. This issue has been patched in version 0.5.0.	5.3	More Details
CVE-2026-81269	Missing Authorization vulnerability in Drupal Data field allows Forceful Browsing. This issue affects Data field versions: from 0.0.0 to 2.0.13.	5.3	More Details
CVE-2026-78149	The Smart Post WordPress plugin before 4.0.8 does not check whether a post is password protected before returning its content and its stored password through an unauthenticated AJAX action, allowing unauthenticated users to read protected post content and the password that guards it.	5.3	More Details
CVE-2025-15489	The Passster WordPress plugin before 4.2.24 does not handle input properly in an AJAX action, allowing unauthenticated users to retrieve the value of password protected content	5.3	More Details
CVE-2026-85701	A vulnerability has been found in ramon-victor freegpt-webui up to 098db3dfeb41555c2ca9269df0f13e10ec1c35dc. This issue affects the function ChatCompletion.create of the file g4f/__init__.py of the component Authentication Check. Such manipulation leads to missing authentication. The attack may be performed from remote. The exploit has been disclosed to the public and may 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. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-81166	Missing Authorization vulnerability in Drupal Digital Signage Framework allows Forceful Browsing. This issue affects Digital Signage Framework versions: from 0.0.0 to 2.6.1.	5.3	More Details
CVE-2026-84379	HTTPX2 is a next generation HTTP client for Python. Prior to 2.11.0, FileField.render_headers() in src/httpx2/httpx2/_multipart.py directly interpolates attacker-controlled content_type values and custom headers from the files= three-element (filename, content, content_type) tuple and the files= four-element (filename, content, content_type, headers) tuple into multipart/form-data part headers without validating header names or values. CR or LF characters can terminate a part header, inject additional part headers, or end the part header block early, allowing a downstream multipart parser to treat attacker-supplied lines as genuine headers and potentially alter part semantics or bypass header-based checks. This issue is fixed in version 2.11.0.	5.3	More Details

CVE-2026-84839	A vulnerability was determined in tsi-coop tsi-dpdp-cms up to 0.5.0. Affected by this issue is some unknown functionality of the file web.xml of the component Admin Console/DPO Compliance Console. Executing a manipulation can lead to missing authentication. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.5.1 can resolve this issue. It is suggested to upgrade the affected component.	5.3	More Details
CVE-2026-82521	parsedmarc 9.0.6 before 11.0.1 writes forensic report sample files using an output path derived from the email subject. When the subject consists entirely of path traversal sequences, the filename sanitization function produces an empty string, and a fallback to the raw unsanitized subject causes the resulting file to be written outside the intended samples directory. An attacker who can cause a forensic failure report with a crafted Subject to be processed can write a dot-prefixed file with attacker-controlled content to an ancestor directory of the configured samples output path. Exploitation requires that file output for forensic report samples is enabled.	5.3	More Details
CVE-2026-73478	Incorrect Authorization vulnerability in Drupal Diff allows Forceful Browsing. This issue affects Diff versions: from 0.0.0 to 2.0.1, from 2.1.0 to 2.1.1.	5.3	More Details
CVE-2025-15481	The Notification Bar for WordPress plugin through 1.1.8 exposes an unauthenticated CSV export script that discloses all stored subscriber emails.	5.3	More Details
CVE-2026-85307	Insertion of Sensitive Information Into Sent Data vulnerability in Kevin Pirnie KP Agent Ready allows Retrieve Embedded Sensitive Data. This issue affects KP Agent Ready: from n/a before 1.2.08.	5.3	More Details
CVE-2026-84856	A vulnerability was detected in rowboatlabs rowboat up to 0.9.1. The impacted element is the function request.text/req.json of the file apps/rowboat/app/api/composio/webhook/route.ts of the component Composio Webhook Endpoint. The manipulation results in denial of service. It is possible to launch the attack remotely. The exploit is now public and may be used. Upgrading to version 0.9.2 is sufficient to resolve this issue. Upgrading the affected component is recommended. The legacy Next.js app was deleted at 0.9.2 rather than patched, leaving no security control behind.	5.3	More Details
CVE-2026-73477	Incorrect Authorization vulnerability in Drupal Quick Tabs allows Forceful Browsing. This issue affects Quick Tabs versions: from 0.0.0 to 4.3.1.	5.3	More Details
CVE-2026-86321	A vulnerability was found in java-json-tools jackson-coreutils 2.0. Affected by this issue is the function JsonLoader.fromURL of the file src/main/java/com/github/fge/jackson/JsonLoader.java of the component URL Validation. The manipulation results in server-side request forgery. It is possible to launch the attack 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.	5.3	More Details
CVE-2026-82056	A race condition in MongoDB server's text index query parsing can cause a heap use-after-free read when handling upsert retry paths. Under certain concurrent index lifecycle operations, a raw pointer to internal text index metadata may be dereferenced after the underlying structures have been freed, leading to a server crash. An authenticated user with readWrite privileges can trigger this condition through specific concurrent text-search and index management operations, resulting in denial of service for all connected clients. This	5.3	More Details
CVE-2026-86319	A vulnerability has been found in java-json-tools json-patch up to 1.13. Affected by this vulnerability is the function JsonPatch.apply of the file src/main/java/com/github/fge/jsonpatch/JsonPatch.java of the component Patch Operation Handler. The manipulation leads to resource consumption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-86318	A flaw has been found in java-json-tools json-patch up to 1.13. Affected is the function JsonMergePatch.fromJson of the file JsonMergePatchDeserializer.java. Executing a manipulation can lead to stack-based buffer overflow. 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.	5.3	More Details
CVE-2026-86317	A vulnerability was detected in ggml-org llama.cpp up to 0.4.0. This impacts the function rpc_server::deserialize_tensor of the file ggml/src/ggml-rpc/ggml-rpc.cpp of the component RPC Server. Performing a manipulation of the argument ne results in reachable assertion. The attack is possible to be carried out remotely. The reported GitHub issue was closed automatically due to inactivity.	5.3	More Details
CVE-2026-81158	Incorrect Authorization vulnerability in Drupal Entity API allows Forceful Browsing. This issue affects Entity API versions: from 0.0.0 to 1.8.0.	5.3	More Details
CVE-2026-	The Accept Stripe Payments WordPress plugin before 2.1.4 does not verify that the product fulfilled when a checkout is completed matches the product the authoritative payment was actually made for, checking only that the amount paid is at least the referenced product's price, allowing unauthenticated attackers who	5.3	More

81424	complete a genuine payment to obtain fulfilment for a different, equal- or lower-priced product than the one they paid for.		Details
CVE-2025-15490	The Passster WordPress plugin before 4.2.26 has a flaw in its global protection checks, allowing unauthenticated users to bypass the protection offered via crafted URLs	5.3	More Details
CVE-2026-4945	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.1.7 via the 'watch_checkout' function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to pay for a lower-cost product while obtaining entitlement for a premium product by manipulating the product_id parameter independently of the price_id parameter in the Stripe checkout URL.	5.3	More Details
CVE-2026-85308	Authorization Bypass Through User-Controlled Key vulnerability in Brainstorm Force SureForms allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SureForms: from n/a through 2.12.5.	5.3	More Details
CVE-2026-81162	Insertion of Sensitive Information Into Sent Data vulnerability in Drupal DXPR Builder: The Best Editing (AI) Experience for Drupal allows Forceful Browsing. This issue affects DXPR Builder: The Best Editing (AI) Experience for Drupal versions: from 0.0.0 to 2.8.1.	5.3	More Details
CVE-2026-85636	A vulnerability was identified in jofpin trape 1.0.0. Affected by this vulnerability is an unknown functionality of the file core/stats.py of the component Login Endpoint. The manipulation leads to missing authentication. The attack may be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2025-8945	The Wp Edit Password Protected WordPress plugin before 1.3.5 allows protecting page content, but this protection can be bypassed by using the REST API.	5.3	More Details
CVE-2026-56101	OpenBSD before commit 1ee99df contains an inverted comparison vulnerability in the ieee80211_michael_mic_failure() function within sys/net80211/ieee80211_crypto_tkip.c that allows unauthenticated attackers within RF range to trigger denial of service by sending two malformed TKIP frames separated by more than 60 seconds. Attackers can exploit the reversed TKIP MIC failure countermeasure window check to deauthenticate all associated TKIP stations and block reassociation for up to 90 seconds, while within-window MIC failures that should engage countermeasures are silently discarded, leaving key-recovery attempts undetected.	5.3	More Details
CVE-2026-84968	An out-of-bounds read in the BSON decoding component of the MongoDB PHP driver may allow an unauthenticated party who supplies specially formed input to have a small amount of adjacent process memory copied into an error message that is returned to application code. This may result in unintended disclosure of limited memory contents.	5.3	More Details
CVE-2026-73474	Server-Side Request Forgery (SSRF) vulnerability in Drupal Entity Share Websub allows Server Side Request Forgery. This issue affects Entity Share Websub versions: from 0.0.0 to 1.1.2.	5.3	More Details
CVE-2026-77782	The Rank Math SEO WordPress plugin before 1.0.277.1 does not check whether a post is password protected before using its content to build publicly generated SEO metadata, allowing unauthenticated users to read the content of password-protected posts.	5.3	More Details
CVE-2026-79631	The WPFunnels WordPress plugin before 3.13.0 does not restrict access to the log files it writes to a predictable location under the public uploads directory, allowing unauthenticated users to download customer order details and opt-in form submissions when logging is enabled.	5.3	More Details
CVE-2026-27347	Missing Authorization vulnerability in Crocoblock JetPopup allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects JetPopup: from n/a through 2.0.20.2.	5.3	More Details
CVE-2026-16966	The Solace Extra WordPress plugin before 1.7.0 does not perform any authorization or post-status checks in one of its AJAX actions, allowing unauthenticated visitors to read the content of non-published (draft, pending, private, and trashed) Site Builder parts that WordPress would otherwise not serve.	5.3	More Details
CVE-2026-84936	The EmbedPress WordPress plugin before 4.6.4 does not have proper authorization on a public review-loading action, allowing unauthenticated users to force the site to make repeated billable third-party API requests using the site's own configured API key, and to create an unbounded number of attacker-controlled rows in the database.	5.3	More Details
CVE-2026-	The MotoPress Appointment Booking WordPress plugin before 2.4.8 does not perform an authorization or ownership check when handling a user-supplied booking identifier on an unauthenticated endpoint, allowing unauthenticated attackers to permanently delete other users' reservations. This is an incomplete fix of CVE-	5.3	More Details

15232	2026-9180: the deletion remains reachable on sites using payment confirmation, confirmed through version 2.4.7.		
CVE-2022-51008	PocketMine-MP before 4.12.3 fails to limit unauthenticated sessions, allowing attackers to exhaust player slots by creating sessions without sending LoginPacket. Attackers can flood the server with unauthenticated connections that occupy max-player slots, preventing legitimate players from joining.	5.3	More Details
CVE-2026-84045	The E-cab Taxi Booking Manager for Woocommerce WordPress plugin before 2.0.5 does not validate a client-supplied trip distance and base-price value on the server before pricing a booking, allowing unauthenticated attackers to manipulate the order total down to zero and place real taxi-booking orders at an arbitrary price.	5.3	More Details
CVE-2026-78151	The FormLayer WordPress plugin before 1.0.9 does not perform any authorization check before returning a form's full stored configuration in the response to its public submission handler, allowing unauthenticated users to disclose notification recipient addresses, confirmation redirect targets and integration settings, including those of unpublished forms.	5.3	More Details
CVE-2026-79632	The WPFunnels WordPress plugin before 3.13.0 does not perform any authorisation or nonce check in one of its opt-in submission handlers, and takes the notification recipients and subject from the request, allowing unauthenticated users to make the site send emails to arbitrary recipients with an arbitrary subject.	5.3	More Details
CVE-2026-84329	Confused deputy in CredentialProvider in Google Chrome on on Windows prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to leak sensitive information via a crafted HTML page. (Chromium security severity: Low)	5.3	More Details
CVE-2026-78153	The Restrict User Access WordPress plugin before 2.8.1 does not normalise the REST API route before checking it against the routes its content protection covers, allowing unauthenticated users to bypass that protection and read restricted content and enumerate users.	5.3	More Details
CVE-2026-86274	A security vulnerability has been detected in projeto-siga siga up to 11.0.2.10/11.0.2.13/11.1.1. This affects the function ExAutenticacaoController.autenticar of the file sigaex/src/main/java/br/gov/jfrj/siga/vraptor/ExAutenticacaoController.java of the component Authentication Flow. Such manipulation of the argument cod/jwt leads to missing authorization. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-86237	A vulnerability was found in openagents-org openagents up to 0.8.19/0.9.3.post20. Impacted is the function test_default_model of the file sdk/src/openagents/sdk/transports/http.py. Performing a manipulation of the argument base_url results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be used. Endpoint and both sinks unchanged since filing; only the file moved (e277dd1a). Maintainer closed as inapplicable yet the identical unguarded code still ships in 0.9.3.post20. Sibling admin endpoints do call the shipped-but-unused-by-this-handler _require_admin().	5.3	More Details
CVE-2026-14350	IBM Cloud Pak for Data System 11.3.0.2 through Interim Fix 001 could allow an unauthorized user to inject data into log messages due to improper neutralization of special elements when written to log files.	5.3	More Details
CVE-2026-79630	The WPFunnels WordPress plugin before 3.13.0 does not verify that the product requested through a checkout order bump is the product that bump's discount was configured for, allowing unauthenticated users to obtain any purchasable product at a discount intended for a different one, with the reduced price carried through to the total of the order they place.	5.3	More Details
CVE-2026-16660	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to cause a denial of service due to an out-of-bounds read.	5.3	More Details
CVE-2026-85157	WWBN AVideo contains a broken access control vulnerability in the unauthenticated feed/index.php endpoint that disables per-video visibility checks when a program_id parameter is supplied. Attackers can enumerate playlist identifiers and retrieve unlisted and group-restricted videos by requesting the RSS feed with any visible playlist id, including empty playlists that return the entire site's hidden video catalogue.	5.3	More Details
CVE-2026-20503	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01371002; Issue ID: MSV-9020.	5.3	More Details
CVE-2026-16826	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	5.3	More Details
CVE-2026-84323	Missing authorization in FileSystem in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process and leveraged social engineering to obtain sensitive information via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details

CVE-2026-20504	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00755024; Issue ID: MSV-7865.	5.3	More Details
CVE-2026-19251	The Ultimate Member WordPress plugin before 2.13.0 does not check whether a comment has been approved, or whether the profile it belongs to is private, before returning profile activity to unauthenticated visitors, allowing them to read the content of comments still awaiting moderation.	5.3	More Details
CVE-2026-86252	h3 versions before 1.15.9 fail to sanitize carriage return characters in EventStream data and comment fields, allowing attackers to inject arbitrary SSE events by including unsanitized carriage returns. Attackers can inject event type directives, split single push calls into multiple browser-parsed events, or escape comment fields to inject data, bypassing the prior CVE fix that only addressed newline injection.	5.3	More Details
CVE-2026-86302	A vulnerability was found in code-projects Hospital Information System 1.0. Affected by this vulnerability is an unknown functionality of the file /HIS/his.sql of the component SQL Database Backup File Handler. Performing a manipulation results in information disclosure. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	5.3	More Details
CVE-2026-84767	Unauthenticated Bypass Vulnerability in BookIt <= 2.6.0.3 versions.	5.3	More Details
CVE-2026-84963	An incorrect numeric conversion in the JSON parsing component of the MongoDB C Driver's BSON library may cause an unusually large text value to be silently shortened, or the corresponding field to be omitted, while the parsing operation still reports success and returns no error. An unauthenticated party who can supply the input processed by an application that uses this component may cause that application to hold data that does not match what was submitted, which may result in unintended alteration of data.	5.3	More Details
CVE-2026-74927	The MultiVendorX WordPress plugin before 5.0.15 does not have proper authorisation controls on one of its REST API listing routes, allowing unauthenticated users to retrieve vendor contact and payout details, pending payout amounts, and administrative notes attached to store applications.	5.3	More Details
CVE-2026-85311	Missing Authorization vulnerability in Kings Plugins MarketKing allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MarketKing: from n/a through 2.1.60.	5.3	More Details
CVE-2026-62652	A vulnerability has been identified in Reyrolle 7SR5 (All versions < V2.70). The device firmware contains binaries from which debugging symbols have not been removed. This could allow an unauthenticated attacker with access to the publicly available firmware update files to more easily reverse engineer the device's firmware, facilitating the identification of further vulnerabilities.	5.3	More Details
CVE-2026-84760	Unauthenticated Broken Access Control in Ultimate Gift Cards For WooCommerce <= 3.2.9 versions.	5.3	More Details
CVE-2026-86284	A security vulnerability has been detected in jaychouchannel Tourism-Management-System up to 8122bf020d91199eddfff3ee02d1632a70a9a132. Affected by this vulnerability is the function getOption of the file travel/src/main/java/com/controller/CommonController.java. The manipulation of the argument tableName/columnName leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed publicly 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 identifier of the patch is d44ec3aa0bd2a72c8800e3befb0a9a96a6491b86. To fix this issue, it is recommended to deploy a patch.	5.3	More Details
CVE-2026-84771	Unauthenticated Insecure Direct Object References (IDOR) in PublishPress Permissions <= 4.8.3 versions.	5.3	More Details
CVE-2026-32480	Missing Authorization vulnerability in WC Lovers WCFM Membership allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WCFM Membership: from n/a through 2.11.11.	5.3	More Details
CVE-2026-85528	Improper input validation of the auto-configuration account identifier in Snowflake JDBC Driver versions 4.2.0 through 4.3.3 allowed a credential-bearing login request to be redirected to an attacker-selected HTTPS endpoint. An attacker able to control the account value could cause the driver to transmit a reusable login credential to a host of their choosing and replay it to obtain the privileges granted to that credential. Successful exploitation requires an application using jdbc:snowflake:auto with a connections.toml section that omits an explicit host and a lower-trust principal able to set the account value; ordinary JDBC URLs are unaffected. The fix is available in Snowflake JDBC Driver version 4.3.4. Users must manually upgrade.	5.3	More Details
CVE-	A vulnerability was found in code-projects Student Crud Operation 1.0. This impacts an unknown function of		More

2026-86519	the file /card_activation.sql of the component Backup File Handler. The manipulation results in information disclosure. The attack can be launched remotely. The exploit has been made public and could be used.	5.3	Details
CVE-2026-86280	A vulnerability was identified in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. This affects an unknown function of the file cict_portal.sql. Such manipulation leads to cleartext storage of sensitive information. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	5.3	More Details
CVE-2026-86513	A security flaw has been discovered in java-json-tools jackson-coreutils 2.0. This vulnerability affects the function TreePointer.tokensFromInput of the file src/main/java/com/github/fge/jackson/jsonpointer/TreePointer.java of the component JSON Pointer parser. The manipulation results in allocation of resources. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-86511	A vulnerability was found in java-json-tools jackson-coreutils 2.0. Affected by this vulnerability is the function BigDecimal.toPlainString of the file src/main/java/com/github/fge/jackson/JacksonUtils.java. Performing a manipulation results in resource consumption. The attack may be initiated 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.	5.3	More Details
CVE-2026-84775	Unauthenticated Denial of Service Attack in Really Simple SSL <= 9.8.0 versions.	5.3	More Details
CVE-2026-86217	A vulnerability was detected in code-projects Hotel and Tourism Reservation in PHP 1.0. Affected is an unknown function of the file /ht/hotel_db%20(1).sql of the component Database Backup Handler. The manipulation results in information disclosure. The attack may be launched remotely. The exploit is now public and may be used.	5.3	More Details
CVE-2026-84043	The ePayco Payment Gateway for WooCommerce WordPress plugin before 8.4.7 does not properly verify the authenticity of payment confirmation requests, allowing unauthenticated attackers to mark orders as paid without a valid gateway signature.	5.3	More Details
CVE-2026-84044	The Restaurant Menu and Food Ordering WordPress plugin before 2.4.12 does not verify that a PayPal payment notification genuinely originates from PayPal, allowing unauthenticated attackers to forge a payment notification and mark their own order as paid and completed without making any payment.	5.3	More Details
CVE-2026-84780	Unauthenticated Denial of Service Attack in WP Go Maps <= 10.1.08 versions.	5.3	More Details
CVE-2026-84146	The Xpro Addons — 140+ Widgets for Elementor WordPress plugin before 1.7.8 does not perform any capability or post-status check before rendering a WooCommerce product summary from a supplied product identifier, allowing unauthenticated visitors to retrieve the title, price, SKU, description and stock details of products that are not publicly published (draft, pending, private or scheduled status).	5.3	More Details
CVE-2026-86275	A vulnerability was detected in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. This vulnerability affects the function register of the file auth.php. Performing a manipulation of the argument role results in improper privilege management. Remote exploitation of the attack is possible. The exploit is now public and may be used.	5.3	More Details
CVE-2026-71216	PagerDuty alarm hook transmits the integration routing key over cleartext HTTP. PagerDuty serves this endpoint over HTTPS and will normally answer plain HTTP with a redirect. That does not remove the exposure. The initial POST -- including the JSON body containing the routing key -- is written to the socket unencrypted before any redirect response is received. Redirection affects only whether the request is retried securely, not whether the first copy left the host in the clear. This issue affects Apache SkyWalking: from 9.6.0 through 11.0.0. Users are recommended to upgrade to version 11.0.0, which fixes the issue.	5.3	More Details
CVE-2026-78543	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a remote attacker to cause a denial of service due to an infinite loop.	5.3	More Details
CVE-2026-81197	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.46 does not restrict access to a REST route that lists an author's courses, nor does it filter that listing by publication status, allowing unauthenticated users to read the titles and IDs of unpublished (draft, pending and private) courses.	5.3	More Details
CVE-2026-86179	A flaw has been found in code-projects Daily Expense Manager 1.0. Affected is an unknown function of the file /Daily-Expense-Manager/exp_ak.sql of the component Database Backup Handler. Executing a manipulation can lead to information disclosure. It is possible to launch the attack remotely. The exploit has been published and may be used.	5.3	More Details
	The B2BKing — Ultimate WooCommerce B2B and Wholesale Plugin — Wholesale Prices, Bulk Order Form &		

CVE-2026-85038	More WordPress plugin before 5.2.40 does not verify that a role selected during registration is one actually offered on the registration form, allowing unauthenticated users to assign themselves to restricted B2B customer groups and to skip the manual account-approval workflow during self-registration.	5.3	More Details
CVE-2026-84762	Unauthenticated Bypass Vulnerability in WP EasyPay <= 4.5.3 versions.	5.3	More Details
CVE-2025-15691	The WPFunnels WordPress plugin before 3.13.0 does not check whether user registration is enabled on the site before creating accounts from opt-in form submissions, relying on a value supplied in the request instead, allowing unauthenticated attackers to create WordPress user accounts even when registration is disabled. This is an incomplete fix for CVE-2025-12353: the check added in 3.6.3 covers only one of the three registration paths.	5.3	More Details
CVE-2026-81195	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.46 does not perform an authorization check before returning per-student course enrollment and progress data, allowing unauthenticated attackers to disclose the enrolled courses and learning progress of any registered user.	5.3	More Details
CVE-2026-83533	The WP Express Checkout WordPress plugin before 2.4.9 does not verify server-side that a payment was actually completed before marking an order as paid, allowing unauthenticated users to forge a completed order without paying.	5.3	More Details
CVE-2026-85517	A flaw has been found in code-projects Vehicle Management System 1.0. The impacted element is an unknown function of the file /vehicle_management.sql of the component SQL Database Backup File Handler. Executing a manipulation can lead to information disclosure. It is possible to launch the attack remotely. The exploit has been published and may be used.	5.3	More Details
CVE-2026-85522	A vulnerability was detected in valkey-io valkey up to 9.5.4/9.1.0. Affected by this vulnerability is the function createSlotImportJob of the file src/cluster_migrateslots.c of the component Slot Migration. The manipulation of the argument job_name results in out-of-bounds read. The attack can be executed remotely. The exploit is now public and may be used. Upgrading to version 9.0.5 and 9.1.1 addresses this issue. The patch is identified as f4dc3ca09eb650c2fe14060090a41c524eca803f. Upgrading the affected component is advised.	5.3	More Details
CVE-2026-82063	A use-after-free security issue in the cursor management component of MongoDB Server allows an authenticated user to cause a denial of service. Under specific timing conditions during cursor operations, a stale pointer to a freed resource may be retained and subsequently dereferenced during cursor cleanup, leading to a server process crash.	5.3	More Details
CVE-2026-77793	The RegistrationMagic WordPress plugin before 6.0.9.9 does not validate the total price of a paid registration server-side, allowing unauthenticated users to complete a paid registration without paying and obtain an activated account.	5.3	More Details
CVE-2026-85662	Marqo 2.26.0 contains a server-side request forgery vulnerability in the add_documents endpoint that allows unauthenticated attackers to trigger requests to arbitrary URLs by supplying malicious media field values. Attackers can exploit download_image_from_url and fetch_content_sample functions which lack destination filtering and host validation to access internal services and cloud metadata endpoints.	5.3	More Details
CVE-2026-85156	WWBN AVideo fails to properly validate access controls on the public channel page, allowing unauthenticated visitors to view unlisted and group-restricted videos through hardcoded visibility flags and an undefined property. Attackers can access the channel endpoint to retrieve sensitive video content that should be hidden, including full URLs to unlisted videos and thumbnails of member-only content, regardless of the operator's hidePrivateVideos setting.	5.3	More Details
CVE-2026-85622	AppFlowy-Cloud through 0.9.64 fails to validate workspace membership when establishing WebSocket connections in the establish_ws_connection_v2 handler, allowing authenticated users to bind sessions to workspaces they do not belong to. Attackers can send sync Manifest messages with victim object identifiers to read full document or database state from collaborations in other workspaces without victim involvement.	5.3	More Details
CVE-2026-85149	SmartIT Desktop Manager developed by Lightstar has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can obtain the SFTP service credentials of the SmartIT Agent application from the source code, thereby browsing the file system of the user's host.	5.3	More Details
CVE-2026-82059	An internal aggregation expression in MongoDB Server was incorrectly registered as accessible to any authenticated user rather than being restricted to internal cluster operations. By crafting a malformed index specification within this expression, an authenticated user with read-only privileges could trigger an assertion failure in the index key generation code path. In certain build configurations, this assertion failure results in termination of the mongod process, causing a denial of service to all connected clients.	5.3	More Details
CVE-2026-85605	Slink before 1.12.3 fails to properly authorize access to image comment endpoints, allowing unauthenticated attackers to read comment threads via GET /api/image/{imageId}/comments and server-sent-events subscriptions. Attackers who obtain image IDs out of band can retrieve full comment threads on public images and subscribe to live comment updates without authentication or authorization checks.	5.3	More Details

CVE-2026-81199	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.46 does not perform an authorization check before returning a student's learning statistics, allowing unauthenticated attackers to disclose the course counts, points, certificates, quiz and assignment totals of any registered user.	5.3	More Details
CVE-2026-17563	The User Frontend WordPress plugin before 4.3.11 does not enforce its subscription-purchase requirement when processing frontend post submissions, only when rendering the form, allowing unauthenticated users to create and, depending on the form's configuration, immediately publish posts through forms restricted to paying subscribers.	5.3	More Details
CVE-2026-50554	Note Mark is an open-source note-taking application. Prior to version 0.19.5, GET /api/books/{bookID}/notes is an unauthenticated endpoint that accepts a "deleted" query parameter. When the request is ?deleted=true, the service runs the query with Unscoped() (bypassing GORM's soft-delete scope) but keeps the read-authorization clause as "owner_id = ? OR is_public = ?". As a result, any unauthenticated caller can enumerate the metadata of soft-deleted ("trashed") notes belonging to any public book — notes the owner explicitly deleted and expected to be removed from public view. This issue has been patched in version 0.19.5.	5.3	More Details
CVE-2026-86239	A vulnerability was identified in liufee FeehiCMS up to 2.1.1. The impacted element is the function UeditorAction::init of the file backend/widgets/ueditor/UeditorAction.php of the component UEditor Widget. The manipulation leads to unrestricted upload. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-77794	The RegistrationMagic WordPress plugin before 6.0.9.9 does not validate a client-supplied quantity multiplier when calculating the total price of a paid registration, allowing unauthenticated users to register without paying and obtain an activated account holding the role the form grants.	5.3	More Details
CVE-2026-17517	The Content Views WordPress plugin before 4.5.1.2 does not check whether the user requesting a view is allowed to read the posts it returns, allowing unauthenticated attackers to obtain the title and content of non-public posts, such as draft, pending, private and scheduled posts, when a view has been configured to include them.	5.3	More Details
CVE-2026-17443	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a remote authenticated attacker to obtain sensitive information due to an XML external entity (XXE) injection flaw.	5.3	More Details
CVE-2026-71222	A heap out-of-bounds read vulnerability was found in gfs2-utils. The ea_num_ptrs field from on-disk extended attribute metadata is consumed without bounds validation, causing a heap buffer over-read that may disclose sensitive memory contents or cause a crash when processing crafted GFS2 filesystem images.	5.3	More Details
CVE-2026-17444	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a remote authenticated attacker to obtain sensitive information due to an XML external entity (XXE) injection.	5.3	More Details
CVE-2026-17469	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to cause a denial of service due to an off-by-one write in the LPD queue name parser.	5.3	More Details
CVE-2026-17470	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to a buffer overflow.	5.3	More Details
CVE-2026-85602	The Grav Form plugin (getgrav/grav-plugin-form) versions 8.0.6 through 9.1.19 select the reCAPTCHA version to validate based solely on which response field key is present in the submitted payload. On a site configured for reCAPTCHA v3, an anonymous attacker can place their v3 token under the v2 field name (g-recaptcha-response instead of token), causing validation to use the v2 branch, which never applies the score threshold or verifies the expected action. This results in a complete bypass of reCAPTCHA v3 bot protection. The issue is fixed in version 9.1.20.	5.3	More Details
CVE-2026-86183	A vulnerability was identified in diem-project diem up to 5.1.3. This vulnerability affects unknown code of the file dmFrontPlugin/modules/dmWidget/lib/BasedmWidgetActions.class.php of the component dmWidget. Such manipulation of the argument widget_id leads to authorization bypass. The attack may be launched remotely. The exploit is publicly available and might be used. The name of the patch is 116974edfb9a5b8bd69cb13586dc62bcdbb485ad. A patch should be applied to remediate this issue. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-19704	The Comments WordPress plugin before 7.6.66 does not validate a value used to build a database query, allowing unauthenticated users to inject SQL and read comments they are not entitled to see, including comments awaiting moderation, comments marked as spam or trashed, and comments on private and draft posts. The injected text reaches the query as grammar rather than as data and does not yield extraction of arbitrary data, so the confidentiality impact is the disclosed comment content rather than the database at large.	5.3	More Details

CVE-2026-78602	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CWE-22) in Elastic Maps Server can lead to information disclosure via Path Traversal (CAPEC-126). An unauthenticated attacker able to reach the service over the network could cause it to return the contents of files outside its intended content directory that are readable by the server process.	5.3	More Details
CVE-2026-53760	Admidio is an open-source user management solution. In versions 5.0.11 and prior, the modules/plugins.php endpoint handles plugin installation, uninstallation, and update operations via GET requests without CSRF token validation. Because these are top-level navigations, browsers include SameSite=Lax session cookies. An attacker crafts a malicious page that, when an authenticated administrator visits it, triggers arbitrary plugin operations. The uninstall operation executes DROP TABLE SQL scripts and destroys plugin data. This issue has been patched via commit 056b1bd.	5.2	More Details
CVE-2026-84966	An incorrect numeric type conversion in the BSON document building component of the MongoDB C++ Driver may cause a length value to be interpreted incorrectly. When an application supplies an extremely large, non-terminated field name to the builder, the library may read memory outside the intended buffer and terminate the calling process. No authentication is required, but the calling application must pass the oversized name in a specific form.	5.1	More Details
CVE-2026-84965	An integer wraparound in an allocation size calculation in the BSON library's JSON parsing code can cause a buffer to be released while a following copy operation still writes through the stale pointer. On builds where sizes are 32 bits, an unauthenticated party able to supply a sufficiently large JSON input to an application that links the library may cause that application to terminate unexpectedly, resulting in denial of service.	5.1	More Details
CVE-2026-17442	IBM App Connect Enterprise 13.0.1.0 through 13.0.8.1, and 12.0.1.0 through 12.0.12.28 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 could allow a local attacker to obtain sensitive information due to credentials being written to trace logs in cleartext.	5.1	More Details
CVE-2026-84386	A unverified ownership vulnerability in Fortinet FortiClientWindows 7.4.0 through 7.4.7, FortiClientWindows 7.2 all versions may allow attacker to improper access control via <insert attack vector here>	5.1	More Details
CVE-2026-19301	IBM Langflow OSS 1.0.0 through 1.11.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	5.0	More Details
CVE-2026-35160	Dell SmartFabric OS10 Software, versions prior to 10.5.6.14, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	5.0	More Details
CVE-2026-86115	Sim before 0.8.14 classifies tool requests as internal based on URL prefix matching without scheme normalization, skipping SSRF validation and minting internal authentication tokens. Authenticated workflow authors can bypass external URL validation by supplying paths starting with /api/ in HTTP blocks to reach internal-only endpoints like POST /api/function/execute.	5.0	More Details
CVE-2026-63694	Dell SmartFabric OS10 Software, versions prior to 10.5.6.14, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	5.0	More Details
CVE-2026-86735	snipe-it versions before 8.7.0 contain a server-side request forgery vulnerability in the ExternalUrl validation rule that fails to detect IPv6 transition addresses encoding private IPv4 targets. Attackers with super-admin privileges can configure webhook URLs using NAT64, 6to4, or Teredo transition addresses to bypass SSRF guards and access internal services or cloud metadata endpoints.	5.0	More Details
CVE-2026-4361	The Divi theme for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.27.6. This is due to the `et_pb_set_video_oembed_thumbnail_resolution()` function using `wp_remote_get()` instead of `wp_safe_remote_get()` to fetch a remote image URL, which does not restrict requests to private or reserved IP ranges. This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application server. The response body is not returned to the attacker (blind SSRF), but two oracles exist: a status oracle (the returned URL string differs depending on whether the target responded with HTTP 200) and a timing oracle (response time varies by target reachability).	5.0	More Details
CVE-2026-18238	The rpcap client code that processes a RPCAP_MSG_PACKET message received from the server incorrectly validates its headers. A malicious server can send a crafted message and cause the client to treat up to 20 bytes of the client process memory beyond the end of the buffer as if it was a part of the captured packet.	5.0	More Details
CVE-2026-17631	IBM Langflow OSS 1.0.0 through 1.10.2 could allow a remote authenticated attacker to obtain sensitive information due to a server-side request forgery (SSRF) vulnerability.	5.0	More Details
CVE-2026-	Zohocorp ManageEngine Endpoint Central versions below 11.5.2605.01 are vulnerable to Local privilege	5.0	More

77699	escalation due to loading a dll from an untrusted path.		Details
CVE-2026-86122	Rowboat through 0.9.1 fails to validate custom MCP server and webhook URLs, allowing authenticated users to configure arbitrary destinations. Attackers can point these URLs at internal services and cloud metadata endpoints to perform server-side request forgery and enumerate internal network topology.	5.0	More Details
CVE-2026-84901	The Eventin WordPress plugin before 4.1.22 does not properly check authorization on several of its event-management REST routes, allowing users with contributor-level access and above to change the site's front-page setting to an event they do not own and to create, edit and delete global event and speaker taxonomy terms they should not be able to manage.	4.9	More Details
CVE-2026-52832	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.16.5, Nuclio Dashboard exposes POST /api/functions without authentication by default (NOP auth mode). The spec.handler field (e.g., mymodule:myfunction) is parsed by functionconfig.ParseHandler() which splits on : only — no path validation is applied to the module portion. This issue has been patched in version 1.16.5.	4.9	More Details
CVE-2026-78594	Improper Handling of Highly Compressed Data (CWE-409) in APM Server can lead to a persistent denial of service via Excessive Allocation (CAPEC-130). An authenticated user with write access to source map content could store specially crafted, highly compressed content that exhausts the memory available to APM Server when it is later processed, terminating the process. The condition recurs on every restart until the stored content is removed.	4.9	More Details
CVE-2026-74235	GFI Exinda AI and ClearView before 7.6.5 contains a path traversal vulnerability in the system maintenance configuration download handler. The wcf_handle_download() function accepts parameters prefixed with v_del_ and appends their values directly to the base configuration directory path without sanitizing for directory traversal sequences. An authenticated attacker with Admin privileges can read arbitrary files from the system in the context of root.	4.9	More Details
CVE-2026-53756	Emlog is an open source website building system. Prior to version 2.6.16, Emlog CMS Pro contains a blind SQL injection in User_Model::getUserDataByLogin(). The $account parameter is directly interpolated into SQL queries without any filtering. The vulnerability is reachable through the auth cookie validation path, where $username is extracted from the cookie and passed unfiltered into SQL — guarded only by an HMAC signature that requires AUTH_KEY to forge. This issue has been patched in version 2.6.16.	4.9	More Details
CVE-2026-22575	An improper access control vulnerability in Fortinet FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.10, FortiManager 7.2 all versions, FortiManager Cloud 7.6.2 through 7.6.4, FortiManager Cloud 7.4.1 through 7.4.10, FortiManager Cloud 7.2 all versions may allow an administrator to bypass the approval process for workflow sessions via crafted HTTP or HTTPs requests.	4.9	More Details
CVE-2026-17627	IBM Langflow OSS 1.0.0 through 1.10.2 could allow a remote authenticated attacker to obtain sensitive information and inject messages into workflow history due to improper authorization.	4.9	More Details
CVE-2026-77788	The Rank Math SEO WordPress plugin before 1.0.277 does not verify that the metadata row being updated belongs to the object the user was authorised against, allowing users with the Author role and above to overwrite arbitrary post and user metadata, including that belonging to higher-privileged users.	4.9	More Details
CVE-2026-79943	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains an Improper Validation of Certificate with Host Mismatch vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to protection mechanism bypass.	4.8	More Details
CVE-2026-18986	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Entity Browser allows Stored XSS. This issue affects Entity Browser versions: from 0.0.0 to 2.16.0.	4.8	More Details
CVE-2026-81167	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Address Suggestion allows Cross-Site Scripting (XSS). This issue affects Address Suggestion versions: from 0.0.0 to 1.0.25.	4.8	More Details
CVE-2026-81571	The Brave WordPress plugin before 0.8.8 does not prevent a URL parameter used to pre-fill a form field from being passed to WordPress's shortcode engine, allowing unauthenticated attackers to have arbitrary shortcodes registered on the site executed server-side.	4.8	More Details
CVE-2026-19862	The JetFormBuilder WordPress plugin before 3.6.5.2 does not validate or strip line breaks from address values it sources from submitted form fields before adding them to the headers of the e-mails it sends, allowing unauthenticated users to inject arbitrary e-mail headers, add hidden recipients and spoof the sender. Exploitation requires the site to be configured to take one of the message's addresses from a form field.	4.8	More Details
CVE-2026-80437	The Ninja Forms WordPress plugin from 3.14.10 before 3.15.2 does not prevent shortcodes in request-derived values from being executed when it substitutes them into content it later processes for shortcodes, allowing unauthenticated users to run any shortcode registered on the site.	4.8	More Details

CVE-2026-80439	The Redirection for Contact Form 7 WordPress plugin from 2.2.7 before 3.2.11 does not prevent shortcodes in submitted form values from being executed when it substitutes those values into an action's settings and then processes those settings for shortcodes, allowing unauthenticated users to run any shortcode registered on the site and read its output.	4.8	More Details
CVE-2026-84793	Craft CMS versions from 5.0.0-RC1 before 5.10.11 contain a stored cross-site scripting vulnerability in the site name field that fails to sanitize input. Administrators can inject arbitrary JavaScript payloads in the site name that execute when other users view the control panel settings pages.	4.8	More Details
CVE-2026-19861	The JetFormBuilder — Dynamic Blocks Form Builder WordPress plugin before 3.6.5.2 does not properly sanitise and escape a form field's value before including it in the HTML notification emails it sends, allowing unauthenticated users to inject arbitrary HTML into messages delivered to administrators and other recipients. Whether injected script executes depends on the recipient's mail client, but the injected markup is rendered regardless.	4.7	More Details
CVE-2026-86271	A vulnerability was found in FluentCMS up to 0.0.5. This affects the function GetAccessible of the file src/Backend/FluentCMS.Services/Permissions/PermissionManager.cs. Performing a manipulation results in missing authorization. It is possible to initiate the attack 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.	4.7	More Details
CVE-2026-71219	A stack overflow vulnerability was found in gfs2-utils. The hash table traversal code in metawalk.c uses alloca() with an exponentially-derived size from the untrusted on-disk di_depth field without bounds validation. A crafted GFS2 filesystem image with a large di_depth value causes stack exhaustion and a denial of service when processed by fsck.gfs2, gfs2_edit, or savemeta.	4.7	More Details
CVE-2026-86667	A weakness has been identified in aircheng-org iWebShop-5 up to 5.15. The affected element is the function member_list of the file controllers/member.php. This manipulation of the argument Search causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-71224	A stack overflow vulnerability was found in gfs2-utils. The metadata walk code in metawalk.c uses alloca() with an untrusted inode height value from on-disk metadata without bounds validation, causing stack exhaustion and a denial of service when processing crafted GFS2 filesystem images.	4.7	More Details
CVE-2026-80176	Dell SCG 5.0 Appliance versions prior to 5.36.00.16 and Dell SCG 5.0 Application versions prior to 5.36.00.00, contains a Plaintext Storage of a Password vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure.	4.7	More Details
CVE-2026-85643	A flaw has been found in code-projects Online Shopping System 1.0. Impacted is the function mysqli_query of the file admin/adduser.php. Executing a manipulation of the argument mobile can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	4.7	More Details
CVE-2026-86240	A security flaw has been discovered in liufee FeehiCMS up to 2.1.1. This affects the function catchImage of the file backend/widgets/ueditor/Uploader.php of the component UEditor. The manipulation of the argument source[] results in server-side request forgery. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-85040	A weakness has been identified in ZhongBangKeJi CRMEB up to 6.0.0. Affected by this vulnerability is the function eval of the file /adminapi/system/crontab/save of the component Custom Scheduled Task Feature. This manipulation of the argument customCode causes os command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Vendor documents this as deliberate debug-only behavior. But isSafePhpCode blacklist offers no real RCE containment.	4.7	More Details
CVE-2026-53636	Open edX Platform enables the authoring and delivery of online learning at any scale. Prior to commit 3a5ac85, a security vulnerability has been identified in the Open edX LMS platform's LTI (Learning Tools Interoperability) Provider implementation. The validate_timestamp_and_nonce function in lms/djangoapps/lti_provider/signature_validator.py does not validate OAuth nonces or timestamps, allowing an attacker who captures a valid LTI launch request to replay it an unlimited number of times without detection. This issue has been patched via commit 3a5ac85.	4.7	More Details
CVE-2026-86516	A vulnerability was detected in elenavanengelenmaslova mocknest-serverless 0.9.0. The affected element is an unknown function of the file deployment/aws/shared/github-oidc-role.yaml of the component AWS GitHub OIDC Deployment Helper Script. Performing a manipulation results in improper privilege management. It is possible to initiate the attack remotely. The patch is named 6ab3147282d867c1993f995272750db091c2290b. Applying a patch is the recommended action to fix this issue.	4.7	More Details
CVE-	SAP S/4HANA Finance (Advanced Payment Management) does not perform sufficient Cross-Site Request Forgery protection on certain requests due to this an attacker with low privileges could craft a malicious link		More

2026-76959	or page. If an authenticated victim interacts with it, unintended actions could be triggered on the web server on their behalf. This results in a low impact on confidentiality and integrity. There is no impact on availability.	4.6	Details
CVE-2026-33387	A template injection vulnerability was discovered in the Dashboards functionality due to improper validation of an input parameter. An authenticated user with the required privileges can define a dashboard containing a malicious payload, or a victim can be socially engineered into importing a malicious dashboard. When the victim views or imports the dashboard, the payload executes in their browser context, allowing the attacker to modify application data or disrupt application availability.	4.6	More Details
CVE-2026-86484	In JetBrains YouTrack before 2026.2.18634 angularJS template injection in assignee names led to stored XSS	4.6	More Details
CVE-2026-49509	Out-of-bounds read vulnerability in Samsung Opensource rLottie allows Overread Buffers. This issue affects rLottie: 25648aef19187b3f87f4d9420b8d761453ad4630.	4.4	More Details
CVE-2026-84852	A security vulnerability has been detected in Reader Tools PDF Reader App 98.8 on Android. The affected element is the function ActSplashNew.handleDeeplink of the component File Handler. The manipulation of the argument _display_name leads to path traversal. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details
CVE-2026-16693	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to the use of hardcoded cryptographic constants to obfuscate encryption keys.	4.4	More Details
CVE-2026-20514	In Audio HAL, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11087632; Issue ID: MSV-8244.	4.4	More Details
CVE-2026-49830	DSpace open source software is a repository application which provides durable access to digital resources. Prior to versions 7.6.7, 8.4, 9.3, and 10.0, when ingesting an aggregated ORE resource by URI (using the OAI-ORE Harvester), the ORE Ingestion Crosswalk does not validate the URI scheme. This may allow for local file inclusion via malicious paths like file:///etc/passwd. The attacker MUST already have DSpace collection administrator privileges in order to perform the attack. This issue has been patched in versions 7.6.7, 8.4, 9.3, and 10.0.	4.4	More Details
CVE-2026-18567	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a local attacker to obtain information due to a race condition involving a predictable Unix domain socket path in a world-writable directory.	4.4	More Details
CVE-2026-84431	A vulnerability was detected in AirAsia MOVE App up to 12.47.1 on Android. This issue affects the function com.airasia.core.utils.RealPathUtil.getRealPath of the component com.airasia.mobile. Performing a manipulation of the argument _display_name results in path traversal. The attack requires a local approach. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details
CVE-2026-18073	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to inject parameters into a CL command due to improper neutralization of special elements.	4.4	More Details
CVE-2026-0001	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform valid GPU memory processing operations to access already freed memory. This issue affects Bifrost GPU Kernel Driver: from r41p0 through r49p5, from r50p0 through r51p0, from r54p1 through r54p2; Valhall GPU Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0.	4.4	More Details
CVE-2026-17499	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	4.4	More Details
CVE-2026-20518	In geniezone, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10867524 / ALPS10876355; Issue ID: MSV-6674.	4.4	More Details
CVE-2026-84442	A vulnerability was identified in MapQuest Get Directions App 10.16.1 on Android. This vulnerability affects the function getDataColumn of the file ExpoShareIntentModule.kt of the component com.mapquest.android.ace. The manipulation leads to path traversal. An attack has to be approached locally. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details

CVE-2026-20513	In Audio HAL, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11087533; Issue ID: MSV-8245.	4.4	More Details
CVE-2026-82066	A heap out-of-bounds read security issue exists in the query planning component of MongoDB Server. An authenticated user with database read and write privileges can trigger the security issue through crafted query operations, causing the server to read memory beyond allocated buffer boundaries. The revealed memory contents may be partially observable through diagnostic query statistics output.	4.3	More Details
CVE-2026-86244	A security vulnerability has been detected in FastAdmin up to 1.2.0.20210401_beta. Affected is the function register/login of the file application/index/controller/User.php of the component User Controller. Such manipulation of the argument url leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. Upgrading to version 1.2.1.20210731_beta is able to address this issue. The name of the patch is b3d32e2bf3637488cfe2fc58a27a9d2475b2b51b. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2026-85107	A vulnerability was found in NousResearch hermes-agent 0.18.0. This vulnerability affects the function resourceBufferFromUrl of the file apps/desktop/electron/main.ts of the component Electron Main Process. Performing a manipulation results in allocation of resources. The attack may be initiated remotely. copyImageFromUrl() entry point no longer reachable on current main. That function did exist at v2026.8.3 but was removed by v2026.8.19. The modern copy-image path is Electron-native event.sender.copyImageAt().	4.3	More Details
CVE-2026-53683	reset_password.html parses query string parameters and uses the 'url' parameter as a redirection target (window.location = url) after password reset, optionally delayed by a 'delay' parameter. No validation or allowlisting is performed on url, enabling an attacker to redirect users to an arbitrary external site after completion of the password-reset workflow.	4.3	More Details
CVE-2026-86241	A weakness has been identified in liufee FeehiCMS up to 2.1.1. This impacts an unknown function of the file environments/prod/backend/config/main-local.php of the component Cookie Validation. This manipulation of the argument cookieValidationKey causes use of hard-coded cryptographic key . The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-75018	The Custom Contact Forms plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 7.16. 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 permanently force-delete arbitrary posts of any post type (including pages, administrator-authored posts, and WooCommerce products) and write arbitrary ccf_field_* post meta onto any post regardless of ownership or post type. The top-level form ID is checked via edit_post/publish_posts, but the nested fields[].ID and choices[].ID paths processed by _create_and_map_fields() and _create_and_map_choices() carry no equivalent capability or post-type guard, leaving those sinks fully exposed while delete_item() and delete_submission() contain explicit post-type restriction fixes demonstrating the developer's awareness of scoping requirements.	4.3	More Details
CVE-2026-84799	Craft CMS before 5.11.0 fails to enforce user-group scope filters on native GraphQL user relations including author, authors, uploader, draftCreator, and revisionCreator fields. Attackers with a scoped GraphQL token can query these relations to read usernames, email addresses, and full names of any content author or uploader including administrators.	4.3	More Details
CVE-2026-13159	The Real Estate Papi WordPress theme through 1.0.5 does not perform capability or CSRF checks on one of its AJAX actions, allowing any authenticated user, such as a subscriber, to install a fixed set of companion from the WordPress.org repository. Where the request runs in the session of a user who can activate , those are activated as well.	4.3	More Details
CVE-2026-86264	A flaw has been found in sfturing ssm_pro up to 627f426331da8086ce8fff2017d65b1ddef384f8. Affected is an unknown function of the file ssm_pro/src/main/java/cn/sfturing/web/OrderController.java of the component Order Endpoint. This manipulation of the argument hospitalName/officesName/doctorName causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-18313	rpcapd can allocate up to 65536 bytes per each RPCAP_MSG_UPDATEFILTER_REQ or RPCAP_MSG_STARTCAP_REQ message received from the client, but it never frees the memory, so it leaks memory even under normal use. A malicious client can cause the server to leak memory substantially faster.	4.3	More Details
CVE-2022-51011	PocketMine-MP before 4.2.10 fails to validate the total length of incoming chat message blobs before splitting them by newline characters, allowing attackers to send large messages containing many newlines. Malicious clients can send megabyte-sized chat packets and bombard the server with thousands of such messages, causing server lockups lasting seconds or minutes.	4.3	More Details
CVE-	Kimai versions before 2.65.0 contain an authorization bypass vulnerability in the REST API timesheet		

2026-84808	collection endpoint that fails to enforce activity-team access controls. Users with view_other_timesheet permission can list timesheets using activities restricted to teams they do not belong to, bypassing intended data isolation.	4.3	More Details
CVE-2026-86294	A vulnerability has been found in SourceCodester Simple Traffic Offense System 1.0. Affected by this issue is some unknown functionality of the file save-settings.php of the component Settings Update Endpoint. The manipulation of the argument site_name/site_desc leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-85100	A vulnerability was detected in 2FastLabs agent-squad up to 1.1.4. Affected by this vulnerability is the function AgentSquad.routeRequest of the file agent-squad/typescript/src/orchestrator.ts of the component Streaming Agent Response Workflow. The manipulation results in resource consumption. It is possible to launch the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-86118	gonic versions before 0.22.0 fail to validate administrator privileges in the startScan endpoint, allowing any authenticated user to trigger media library rescans. Attackers can repeatedly call the startScan endpoint to force CPU and I/O-intensive filesystem operations, causing denial of service on multi-user instances.	4.3	More Details
CVE-2026-85021	A vulnerability was determined in langgenius dify 1.13.0. Affected is the function router.replace of the file web/app/(shareLayout)/components/splash.tsx of the component Splash Layout. This manipulation of the argument redirect_url causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-86216	A security vulnerability has been detected in code-projects Hotel and Tourism Reservation in PHP 1.0. This impacts an unknown function of the file /ht/details.php. The manipulation of the argument room leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-86120	APITable through 1.13.0-beta.1 contains an incorrect authorization vulnerability in NodePermissionGuard that fails to enforce node-level access control when permission lookups throw exceptions. Attackers with valid Fusion API tokens can write attachments to private datasheets they have been explicitly denied access to by exploiting the unhandled exception in the permission guard.	4.3	More Details
CVE-2026-86215	A vulnerability was identified in Mstfakts College-Management-System. The affected element is an unknown function of the file Front-end/server.php of the component Logout Handler. Such manipulation of the argument log_out leads to session expiration. It is possible to launch the attack remotely. The exploit is publicly available and might 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.	4.3	More Details
CVE-2026-86174	Plane through 1.4.2 fails to validate that issues belong to the deploy board's project in the public comment endpoint. Authenticated attackers can post comments to arbitrary issues across workspaces by supplying an issue_id parameter to the public deploy-board comment endpoint.	4.3	More Details
CVE-2026-85161	AVideo through commit c91b5975d contains a cross-site request forgery vulnerability in removePoster.php that lacks forbidIfNotPost or forbidIfInvalidToken checks. Attackers can craft malicious image tags to delete authenticated victims' live poster and thumbnail files via GET requests.	4.3	More Details
CVE-2026-86176	NetBox through 4.7.0 fails to properly scope user-private records in REST and GraphQL API endpoints for Notifications, Subscriptions, and Bookmarks. Authenticated users with view permissions can access all users' private records through unscoped querysets, disclosing which users watch or bookmark which objects.	4.3	More Details
CVE-2026-84805	Kimai versions from 2.61.0 before 2.63.0 fail to disable admin-only work-contract preferences for low-privilege users in the PATCH /api/users/{id}/preferences endpoint. Although the web interface gates these employment-contract fields behind the contract_other_profile admin permission, the WorkContractPreferenceSubscriber (introduced in 2.61.0) registers the preferences as enabled without a permission check, so an authenticated regular user can use the API to modify their own admin-only work-contract data. The issue is fixed in 2.63.0 by applying the same permission check to the API endpoint.	4.3	More Details
CVE-2026-86668	A security vulnerability has been detected in aircheng-org iWebShop-5 up to 5.15. The impacted element is the function uploadFile of the file controllers/pic.php. Such manipulation of the argument outerSrc/selectPhoto leads to cross site scripting. The attack may be performed from remote. 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.	4.3	More Details
CVE-2026-84792	Craft CMS versions before 5.10.11 contain a broken access control vulnerability in the element-indexes/save-elements endpoint that allows control panel users to move entries into sections they cannot edit. Attackers with limited section permissions can relocate or publish entries to unauthorized sections by overwriting the sectionId attribute after initial authorization checks, bypassing the destination section permission validation.	4.3	More Details
	A vulnerability was found in Ollama up to 0.31.1. This issue affects the function readGGUFV1String of the file		

CVE-2026-86289	fs/ggml/gguf.go of the component GGUF Decoder. Performing a manipulation results in integer overflow. The attack is possible to be carried out remotely. The exploit has been made public and could be used. Upgrading to version 0.31.2-rc1 is capable of addressing this issue. The patch is named 67b6a1c2d45321e0cb3c04a18073f9818de7724b. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2026-86212	A vulnerability has been found in Open5GS 2.7.7/2.8.0. This vulnerability affects unknown code of the component AMF/MME. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 9468de94caed2fc940f4a23cbf734651896d0fde. To fix this issue, it is recommended to deploy a patch.	4.3	More Details
CVE-2026-86278	A vulnerability was found in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. The affected element is an unknown function of the file manage_subjects.php. The manipulation of the argument msg/title/content results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used.	4.3	More Details
CVE-2026-86228	A security vulnerability has been detected in JeecgBoot up to 3.9.3. This vulnerability affects the function exportXls of the file jeecg-boot/jeecg-boot-module/jeecg-boot-module-airag/src/main/java/org/jeecg/modules/airag/llm/controller/AiragModelController.java. Such manipulation of the argument credential leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 3.9.5 is able to resolve this issue. The name of the patch is a2be896f753936956ee6863b632b8e5a0231345c. You should upgrade the affected component.	4.3	More Details
CVE-2026-15550	The Ninja Forms - Save Progress plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 3.0.30. This is due to the lack of capability checks and nonce verification in the 'bulk_actions' function. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary database records from the 'wp_nf3_objects' table, such as saved submissions.	4.3	More Details
CVE-2026-86238	A vulnerability was determined in projectworlds Online Examination System 1.0. The affected element is an unknown function of the file feedback.php of the component Feedback Form. Executing a manipulation of the argument Name/Subject can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-84802	Craft CMS versions from 5.7.0 before 5.10.12 contain an information disclosure vulnerability in AssetsController::actionMoveInfo that fails to enforce volume permissions. Authenticated control panel users can submit POST requests to the assets/move-info endpoint with arbitrary folderIds to retrieve asset count and total storage size for volumes they cannot access.	4.3	More Details
CVE-2026-86285	A vulnerability was detected in BookStack up to 26.05.2. Affected by this issue is the function AttachmentController::getUpdateForm of the file app/Uploads/Controllers/AttachmentController.php of the component Attachment Edit Endpoint. The manipulation of the argument ID results in improper access controls. The attack may be launched remotely. The exploit is now public and may be used. The patch is identified as 4e406c41c4c8060a5795e74c66fb96362e54f400. It is advisable to implement a patch to correct this issue.	4.3	More Details
CVE-2026-86281	A security flaw has been discovered in SourceCodester Syllabus-Aligned Learning Management & Examination System 1.0. This impacts an unknown function. Performing a manipulation results in cross-site request forgery. 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-2026-86191	SiYuan versions before v3.8.2 contain an information disclosure vulnerability in the getAttributeViewKeysByID endpoint that allows publish readers to enumerate private attribute view key definitions without verifying parent database visibility. Attackers can access the endpoint to retrieve complete key schemas including sensitive field names and relation definitions from hidden databases.	4.3	More Details
CVE-2026-86182	A vulnerability was determined in diem-project diem up to 5.1.3. This affects the function executeCommand of the file dmAdminPlugin/modules/dmConsole/actions/actions.class.php of the component dmConsole. This manipulation of the argument dm_command causes cross-site request forgery. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-78596	Missing Authorization in Kibana Leading to Unauthorized Modification of Data / Missing Authorization (CWE-862) in Kibana can lead to unauthorized modification of data via Privilege Abuse (CAPEC-122). An authenticated user holding Security read-level access in a single Kibana space could trigger Entity Analytics migration operations that perform privileged writes across all Kibana spaces, regardless of that user's actual access scope.	4.3	More Details
CVE-2026-84425	A vulnerability was found in zhayujie CowAgent up to 2.1.3. This impacts the function BrowserTool of the file agent/tools/browser/browser_tool.py of the component Browser Tool. Performing a manipulation results in denial of service. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE-2026-17259	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service due to a stack-based buffer overflow.	4.3	More Details
CVE-2026-84658	Jenkins Script Security Plugin 1412.v7737b_3405f86 and earlier uses the `@DataBoundConstructor` annotation on a constructor that loads script approval configuration, allowing attackers able to submit certain forms to read that configuration.	4.3	More Details
CVE-2026-84659	Jenkins Script Security Plugin 1412.v7737b_3405f86 and earlier does not enforce a permission check in the method that controls the "Force the use of the sandbox globally in the system" setting, allowing attackers to disable it through Stapler data binding.	4.3	More Details
CVE-2026-82309	Robots::Validate versions from 0.3.2 before 0.3.11 for Perl allow unbounded outbound DNS queries per validation via a forward-confirmation loop that does not bound the names it queries. _check_dns issues one PTR query for the client address, keeps the returned names matching the rule's domain, and issues a forward query for each until one resolves back to that address. Nothing bounds that list, and a client controls the reverse zone for its own address, so it chooses how many names the PTR answer holds. Net::DNS refetches a truncated answer over TCP by default, so the 512-byte UDP payload does not cap it either. Any client whose User-Agent matches a rule with a domain reaches _check_dns. Each forward name is distinct and client-chosen, so every query misses the local cache and is resolved against the authoritative servers for that domain. The queries are synchronous, so the caller is held until all of them answer or time out.	4.3	More Details
CVE-2026-86736	snipe-it before 8.7.0 contains an incorrect calculation vulnerability in checkout request handling that allows authenticated users to corrupt the assets.requests_counter through duplicate submissions and cancellations without active requests. Attackers can repeatedly call cancel endpoints without active requests to drive the counter negative, or submit duplicate checkout requests to inflate the counter, misrepresenting pending demand in the admin queue.	4.3	More Details
CVE-2026-84356	UI misrepresentation in FullScreen in Google Chrome prior to 152.0.7977.75 allowed a remote attacker to spoof address bar via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-81432	The JetStyleManager for Gutenberg WordPress plugin before 1.3.9 does not have CSRF protection on some of its AJAX actions, allowing attackers to make a logged-in user with the edit_posts capability (Contributor and above) delete or modify custom widget skins via a crafted request, provided they can trick the user into performing an action such as clicking a link.	4.3	More Details
CVE-2026-79621	The CatalogX WordPress plugin before 6.1.3 does not sanitise or escape content that an unauthenticated user can store before including it in the product enquiry notification email sent to the site administrator, allowing unauthenticated attackers to inject arbitrary content into that email, which is delivered when an unrelated visitor later submits a product enquiry.	4.3	More Details
CVE-2026-85382	A vulnerability was detected in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. Impacted is the function htmlspecialchars_decode of the file App/Home/View/Default/Chapter/oneChapter.tpl of the component Chapter Content Output. Performing a manipulation of the argument content results in cross site scripting. Remote exploitation of the attack is possible. The exploit is now public 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.	4.3	More Details
CVE-2026-84662	Jenkins LDAP Plugin 807.809.vd3a_4e5e4ec98 and earlier allows connecting to a specified URL through Stapler data binding, allowing attackers to connect to an attacker-specified URL.	4.3	More Details
CVE-2026-16941	IBM i 7.6, 7.5, and 7.4 could allow a remote authenticated attacker to modify certain system messages due to improper authorization.	4.3	More Details
CVE-2026-86481	In JetBrains YouTrack before 2026.2.18634 signed URL reuse allowed disclosure of restricted project icons	4.3	More Details
CVE-2026-17255	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to improper validation of the prefix length in ICMPv6 Router Advertisements.	4.3	More Details
CVE-2026-81427	The WC Vendors WordPress plugin before 2.7.2.1 does not verify that the vendor submitting a front-end order shipment status change owns the referenced order, allowing any authenticated vendor to mark another vendor's order as shipped, add an order note falsely attributed to the victim vendor, and trigger the customer shipment notification email.	4.3	More Details
CVE-	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to cause a denial of service due to a stack-based		More

2026-17270	buffer overflow.	4.3	Details
CVE-2026-86496	In JetBrains YouTrack before 2026.2.18769 missing access control on Helpdesk authorized reporters exposed reporter email addresses	4.3	More Details
CVE-2026-17483	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 IBM i could allow a local attacker to delete historical flight-recorder archives due to improper access control in an SQL procedure.	4.3	More Details
CVE-2026-18076	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service due to a memory leak.	4.3	More Details
CVE-2026-18078	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service due to an integer overflow.	4.3	More Details
CVE-2026-84676	Jenkins Parameterized Remote Trigger Plugin 3.2.2 and earlier stores tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details
CVE-2026-81426	The WC Vendors WordPress plugin before 2.7.2.1 does not have CSRF protection on some of its front-end order shipment status actions, which could allow attackers to make a logged-in vendor change the shipment status of their own orders via a crafted request.	4.3	More Details
CVE-2026-85579	SiYuan is affected by an information disclosure vulnerability (confirmed in v3.8.1, fixed in v3.8.2) in the reader-accessible POST /api/transactions/undoState endpoint. The endpoint returns the peekMutatedRootIDs list from the global undo-log stack for a caller-supplied root ID without applying publish-access visibility filtering. An authenticated reader who knows the root ID of a visible document can obtain the internal root IDs of other documents (including private or unpublished ones) modified in the same cross-document transaction, disclosing internal identifiers and cross-document relationships. Document body contents are not directly exposed.	4.3	More Details
CVE-2026-85407	A vulnerability was found in Eleveo Quality Management 9.7.0. This issue affects some unknown processing of the file /enc-fwk-data/api/v3/conversations/<ID>/events of the component Conversation Handler. The manipulation of the argument labels results in denial of service. The attack can be executed remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-85408	A vulnerability was determined in Eleveo Quality Management 9.7.0. Impacted is an unknown function of the file /enc-fwk-data/api/v3/conversations/<ID>/events of the component Conversation Handler. This manipulation of the argument createdBy causes dynamically-determined object attributes. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-19043	Missing Authorization vulnerability in Menulux Software Inc. Menulux Portal allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Menulux Portal: before 20260903211448.	4.3	More Details
CVE-2026-86853	A malicious webpage could repeatedly trigger external URL schemes, causing system prompts or external application launches. This could make Firefox for iOS temporarily unusable until the page is closed. This vulnerability was fixed in Firefox for iOS 155.1.	4.3	More Details
CVE-2026-82298	Incorrect Authorization (CWE-863) in Kibana can lead to denial of service via Exploiting Incorrectly Configured Access Control Security Levels (CAPEC-180).	4.3	More Details
CVE-2026-86737	snipe-it versions before 8.7.0 fail to enforce asset view authorization in the GET /hardware/{asset}/barcode endpoint. Authenticated attackers can iterate asset IDs to retrieve barcodes and enumerate asset tags across tenants, including soft-deleted and cross-company assets.	4.3	More Details
CVE-2026-81194	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.46 does not properly verify authorization when retrieving order line-item data, allowing any authenticated user including Subscribers to read other instructors' course sales records by supplying another user's identifier.	4.3	More Details
CVE-2026-19081	Missing Authorization vulnerability in Gastromenum Gastromenum Ticket and QR Menu System allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Gastromenum Ticket and QR Menu System: before 2026.08.31.	4.3	More Details
CVE-2026-	SAP S/4HANA (Manage Bank Chains app) does not perform sufficient authorization checks within certain affected functionality. An attacker with low privileges could send specially crafted requests to delete specific	4.3	More

76962	entries that should not be accessible to them. This results in a low impact on availability. There is no impact on confidentiality and integrity.		Details
CVE-2026-84833	A vulnerability was found in ntegrals openbrowser up to 067fc45d649baa961750da8e2f4a75d87c5c75c8. Affected by this vulnerability is an unknown functionality of the file packages/core/src/agent/agent.ts of the component Browser Agent Message Construction. Performing a manipulation results in resource consumption. It is possible to initiate the attack remotely. The exploit has been made public and could 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 vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-85210	Oppia's AdminRoleHandler GET endpoint in core/controllers/admin.py is decorated with open_access, allowing any registered user to enumerate privileged accounts and roles. Attackers can query the endpoint with filter_criterion parameters to retrieve usernames holding specific roles, banned flags, and managed topic identifiers without authorization.	4.3	More Details
CVE-2026-78595	Missing Authorization in Kibana Leading to Information Disclosure / Missing Authorization (CWE-862) in the Kibana Fleet feature can lead to information disclosure via Privilege Abuse (CAPEC-122). An authenticated user holding read-level Fleet agent privileges in one Kibana space could enumerate agent metadata and access diagnostic content belonging to agents enrolled in other Kibana spaces.	4.3	More Details
CVE-2026-85392	Peppermint through 0.5.5 contains an authorization bypass vulnerability in the GET /api/v1/auth/user/:id/logout endpoint that allows authenticated attackers to delete sessions for any user by supplying arbitrary user IDs. Attackers can forcibly log out any user including administrators by calling the logout handler with another user's ID, since the endpoint performs no authorization checks to verify the caller owns the target account.	4.3	More Details
CVE-2026-16983	The Gutentor WordPress plugin before 4.0.6 does not apply the correct context restriction to one of its REST endpoints, exposing the plaintext passwords of password-protected posts to any authenticated user with at least the Subscriber role.	4.3	More Details
CVE-2026-81423	The Accept Stripe Payments WordPress plugin before 2.1.4 does not validate a user-supplied URL before using it in a redirect, allowing unauthenticated attackers to redirect visitors to an arbitrary external website, which can be leveraged for phishing.	4.3	More Details
CVE-2026-79603	x86 PV guests can free memory pages while still keeping a stale TLB entry pointing to them. A TLB flush is only issued by Xen (if needed) when the page is re-used. Since it's possible for the page to be scrubbed ahead of the TLB flush, there's a window where a PV guest can modify an already scrubbed page.	4.3	More Details
CVE-2026-84888	A weakness has been identified in RightNow-AI OpenFang up to 0.6.9. This vulnerability affects the function shell_exec of the file crates/openfang-runtime/src/tool_runner.rs. This manipulation causes uncontrolled memory allocation. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-84967	A component of the MongoDB extension for Visual Studio Code does not neutralize special characters in a connection string before that value is placed into a command line the extension composes for an integrated terminal. An unauthenticated remote unauthorized-user who persuades a developer to accept a user-supplied connection target, and then to open the extension's shell feature, can place characters of the unauthorized-user’s choosing into that command line. No privileges on the developer's machine are required, but several user actions are. The confirmation the developer sees does not display the supplied text.	4.3	More Details
CVE-2026-78593	An insufficiently validated configuration field in Kibana's Cribl integration allows an authenticated user holding Kibana Fleet management privileges to inject attacker-controlled expressions into a server-side script template, resulting in an Elasticsearch ingest pipeline being written beyond the caller's authorized Elasticsearch permissions.	4.3	More Details
CVE-2026-83628	The Theme My Login plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 7.1.15 on Multisite installations. This is due to the `tml_ms_signup_handler()` function's `gimmeanotherblog` branch failing to enforce the network's `active_signup` registration policy, checking only `is_user_logged_in()` while sibling branches such as `validate-blog-signup` apply the full policy gate. This makes it possible for authenticated attackers, with Subscriber-level access and above, to directly POST `stage=gimmeanotherblog` to Theme My Login's signup route, bypassing the configured registration policy entirely — even when it is set to `none` or `user` — which causes `wpmu_create_blog()` to execute with the attacker's user ID, after which WordPress core assigns the Administrator role on the newly created subsite via `add_user_to_blog()`. The privilege gain is scoped to the newly created subsite only; the attacker's account retains Subscriber-level access on the main site and does not obtain Super Admin or network-level capabilities such as `manage_network` or `manage_sites`.	4.3	More Details
CVE-2026-78584	Observable Response Discrepancy (CWE-204) in the Kibana Osquery feature can lead to information disclosure via Query System for Information (CAPEC-54). An authenticated user holding Osquery live-query privileges could determine whether a scheduled query identifier exists in a Kibana space they are not authorized to access.	4.3	More Details

CVE-2026-77764	The GamiPress WordPress plugin before 7.9.9.6 does not properly restrict its video watch-tracking functionality, allowing users with a role as low as Subscriber to award the configured gamification points, achievements and ranks to arbitrary users including administrators, and to accrue them without limit.	4.3	More Details
CVE-2026-86515	A security vulnerability has been detected in vgmstream up to r2117. Impacted is the function add_entry of the file src/meta/txtp_parser.c of the component txtp. Such manipulation of the argument range_start/range_end leads to resource consumption. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The name of the patch is 4b6a02dd1aff6428255db912563d77d4cb0a143e. It is advisable to implement a patch to correct this issue.	4.3	More Details
CVE-2026-84887	A vulnerability was identified in simular-ai Agent-S up to 0.3.2. Affected by this issue is some unknown functionality of the file grounding.py of the component Model-generated GUI Action Execution Workflow. The manipulation leads to denial of service. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-82293	Incorrect Authorization (CWE-863) in the Kibana machine learning feature can lead to unauthorized resource consumption via Exploiting Incorrectly Configured Access Control Security Levels (CAPEC-180). An authenticated user could invoke machine learning functionality beyond their authorization scope, consuming cluster resources they should not be able to reach.	4.3	More Details
CVE-2026-84885	A vulnerability has been found in simular-ai Agent-S 0.3.1/0.3.2. This impacts an unknown function of the file code_agent.py of the component CodeAgent. Such manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-85676	Dub contains an open redirect vulnerability in the redir_url query parameter that is accepted on every short link without validation or domain allowlist enforcement. Attackers can append the redir_url parameter to any short link to redirect visitors to arbitrary external URLs through the trusted Dub domain, bypassing destination blacklists and potentially enabling phishing attacks with link cloaking enabled.	4.3	More Details
CVE-2026-84646	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, user objects can appear as nested field values in other deserialized XML objects, allowing attackers with Overall/Read permission to create user objects by submitting crafted XML.	4.3	More Details
CVE-2026-84427	A vulnerability was determined in zhayujie CowAgent up to 2.1.7. Affected is an unknown function of the file agent/tools/bash/bash.py of the component Bash Tool. Executing a manipulation can lead to denial of service. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-84655	Jenkins 2.579 and earlier, LTS 2.568.2 and earlier does not escape map keys when serializing objects as JSON and Python through its REST API, allowing attackers able to control map property names to inject arbitrary fields into JSON and Python API responses.	4.3	More Details
CVE-2026-84656	A missing permission check in Jenkins 2.579 and earlier, LTS 2.568.2 and earlier allows attackers with Item/Read permission on at least one job to read build parameter names and values of jobs they have no access to.	4.3	More Details
CVE-2026-14466	It’s possible to run a stored XSS in Stormshield’s web administration panel. To exploit this vulnerability, a SNS administrator with appropriate permissions must inject some malicious script in a group’s comments in the webservices administration interface.	4.3	More Details
CVE-2026-86307	A security vulnerability has been detected in light0011 cms c774dce31c6df0055568a8d5c53d964d99be199d/f72cf46f601efb2a0618c3814cc2f61380b38930. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. 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.	4.3	More Details
CVE-2026-76977	SAP UI5 does not sufficiently validate the parent frame's origin against the configured allowlist. An unauthenticated attacker could host a malicious page to bypass framing restrictions. If an authenticated victim visits the attacker's page and interacts with it, the attacker could trick the victim into performing unintended actions, resulting in a low impact on integrity. There is no impact on confidentiality and availability.	4.3	More Details
CVE-2026-76963	Due to a missing authorization check in Application Server ABAP of SAP NetWeaver and ABAP Platform, an authenticated attacker could gain unauthorized access to sensitive system configuration information. Successful exploitation could result in exposure of security relevant settings and internal system details, resulting in low impact on confidentiality while integrity and availability remain unaffected.	4.3	More Details
	LearnPress WordPress Plugin before 4.4.6 contains a broken object-level authorization vulnerability that		

CVE-2026-82023	allows authenticated attackers with the Instructor role to add answers to quiz questions owned by other instructors by exploiting a missing ownership check on the question answer insert path. Attackers can supply arbitrary question identifiers during answer insertion, bypassing instructor-boundary restrictions to persistently modify quiz content across courses they do not own.	4.3	More Details
CVE-2026-86499	In JetBrains YouTrack before 2026.1.14047 predefined search fields leaked all group names to any user, regardless of visibility permission	4.3	More Details
CVE-2026-84962	An unauthorized user with key vault write access may cause an authorized client to issue arbitrary authenticated Google Cloud KMS API calls under the authorized user's identity, escalating database-level access into cloud key control and defeating client-side encryption.	4.2	More Details
CVE-2026-84657	In Jenkins 2.579 and earlier, LTS 2.568.2 and earlier, the build CLI command does not check the Item/Cancel permission when using the -s flag to cancel a build triggered to wait for completion, allowing attackers with Item/Build permission to cancel builds started by other users.	4.2	More Details
CVE-2026-84358	Improper privilege management in Downloads in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to spoof address bar via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2026-83543	The Greenshift WordPress plugin before 13.2.0 does not validate a user-supplied URL before fetching it server-side, allowing users with contributor-level access and above to make the server issue requests to arbitrary hosts and read the response.	4.1	More Details
CVE-2026-86150	A security vulnerability has been detected in Tenda CP3 27.5.57.101. Impacted is an unknown function of the file custom-x/softap/hostapd. Such manipulation of the argument wpa_passphrase leads to hard-coded credentials. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.1	More Details
CVE-2026-82182	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.133 does not sanitise a user supplied list of identifiers before using it in a SQL query, allowing administrators to perform SQL injection attacks.	4.1	More Details
CVE-2026-82186	The WPLP Cookie Consent WordPress plugin before 4.4.2 does not properly validate a pagination parameter before using it in a SQL query, allowing users with administrator privileges to perform SQL injection attacks.	4.1	More Details
CVE-2026-16647	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Disable Login Page allows Functionality Bypass. This issue affects Disable Login Page versions: from 0.0.0 to 1.1.4.	4.1	More Details
CVE-2026-74768	Dell PowerProtect Data Manager, versions 20.2.0.0 and below, contain a Server-Side Request Forgery (SSRF) vulnerability in the REST API. A high privileged remote attacker could potentially exploit this vulnerability, leading to Information disclosure.	4.1	More Details
CVE-2026-81198	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.46 does not properly verify ownership of a curriculum object before acting on it, allowing authenticated users with the instructor role to delete or modify curriculum sections and materials belonging to courses owned by other instructors.	3.8	More Details
CVE-2026-14326	The Timetics WordPress plugin through 1.0.61 does not enforce per-object ownership when updating appointments through its REST API, allowing users with its custom staff role to modify, disable, or take over appointments belonging to other staff members.	3.8	More Details
CVE-2026-73318	XenForo before 2.3.13 contains a missing authorization vulnerability in the force-agreement controller that allows any ACP administrator to access and submit force-agreement forms regardless of their assigned permissions. Attackers can bypass the option permission declared in the navigation configuration to update the global policy last-updated timestamp, forcing all users to re-agree to the privacy policy or terms of service.	3.8	More Details
CVE-2026-84947	undici's dump interceptor reads and discards a response body up to a configurable maximum size. When a response declares a Content-Length that exceeds the maximum, the interceptor aborts cleanly, but when a response has no Content-Length and is chunked, the interceptor instead signals completion early once the accumulated size reaches the maximum, without pausing or aborting the request. Because the underlying parser keeps delivering body bytes, a second completion signal fires and trips an internal assertion, which aborts the request and tears down the connection. The application is left observing a misleading successful status with an empty or truncated body while the connection has actually been disconnected. This affects undici versions from 7.1.0 up to 7.29.1 and from 8.0.0 up to 8.10.2. Users should upgrade to undici 7.29.1 or 8.10.2.	3.7	More Details
	undici's retry interceptor can append the body of a ranged retry response to bytes already delivered from an earlier partial response while still presenting the original response's status and headers. This happens when an upstream server delivers part of a body without a trustworthy resume checkpoint, for example a non-		

CVE-2026-18540	success response whose headers were already sent or a partial-content response with an unusable content range, then closes the connection and answers the resumed range request with more bytes. As a result the response body can be longer than the Content-Length that the application observes. An application that relays such a response to a downstream HTTP/1.1 peer without normalizing the framing can emit a body that exceeds the forwarded Content-Length, and the excess bytes can be interpreted as the start of a following response, which enables downstream response splitting or desynchronization. Exploitation requires an attacker-controlled upstream server and an application that forwards the response through a framing-sensitive path. This affects undici versions before 6.28.1, from 7.0.0 up to 7.29.1, and from 8.0.0 up to 8.10.2. Users should upgrade to undici 6.28.1, 7.29.1, or 8.10.2.	3.7	More Details
CVE-2026-81168	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal CAPTCHA Protected Page allows Functionality Bypass. This issue affects CAPTCHA Protected Page versions: from 0.0.0 to 1.0.2.	3.7	More Details
CVE-2026-85704	A security flaw has been discovered in ramon-victor freegpt-webui up to 098db3dfeb41555c2ca9269df0f13e10ec1c35dc. This issue affects the function getJailbreak of the file server/config.py of the component Jailbreak Mode. The manipulation results in race condition. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitability is assessed as difficult. The exploit has been released to the public and may be used for attacks. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. This vulnerability only affects products that are no longer supported by the maintainer.	3.7	More Details
CVE-2026-86486	In JetBrains YouTrack before 2026.2.18634 the generic VCS webhook handler failed open when its secret was blank	3.7	More Details
CVE-2026-81159	Observable Timing Discrepancy vulnerability in Drupal Commerce CyberSource allows Brute Force. This issue affects Commerce CyberSource versions: from 0.0.0 to 1.10.0.	3.7	More Details
CVE-2026-77783	The Rank Math SEO WordPress plugin before 1.0.277 does not verify that the post whose schema it renders on the front end is publicly viewable, allowing unauthenticated visitors to disclose the schema and associated content of draft, pending, private, scheduled and password-protected posts.	3.7	More Details
CVE-2026-84969	A memory-handling error in the BSON-to-JSON conversion helpers of the MongoDB C Driver can write a small number of bytes past the end of a heap buffer when a binary field is encoded and the output is cut short at a caller-configured length limit. A party who supplies the document content, with no privileges on the application that links the driver, may cause a small amount of data outside the intended buffer to be altered.	3.7	More Details
CVE-2026-86420	ImageMagick before 7.1.2-30 and 6.9.13-55 fails to properly lower the memory budget when an operation inside OpenPixelCache fails. Repeated triggering of such failures can exhaust the process memory budget and result in a denial of service.	3.7	More Details
CVE-2026-85592	phpMyFAQ before 4.1.8 contains an authorization bypass vulnerability in the question creation endpoint where the isAddingQuestionsAllowed() method grants access to all callers when main.enableAskQuestions is enabled, ignoring the records.allowQuestionsForGuests setting. Unauthenticated attackers can submit questions via the question/create API endpoint to bypass guest submission restrictions and inject spam into the admin moderation queue.	3.7	More Details
CVE-2026-85030	A vulnerability has been found in HKUDS AI-Trader up to d03ff6c056b32ced735adf7c19ed8175adb1c8df. The affected element is an unknown function of the file service/server/routes_agent.py of the component selfRegister API Endpoint. Such manipulation of the argument initial_balance leads to business logic errors. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is described as difficult. The exploit has been disclosed to the public and may 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. profit_percent_for_display() divides by INITIAL_CAPITAL + deposited, and challenge scoring's return_pct also normalises against the attacker-inflated starting_cash. So an inflated initial_balance does not yield artificial percent returns - it inflates the absolute cash/equity column only, which is a cosmetic/leaderboard-gaming concern in a simulated game.	3.7	More Details
CVE-2026-81348	The My Private Site WordPress plugin before 4.2.3 does not apply its site-privacy access control to certain unauthenticated front-end read surfaces, allowing unauthenticated users to view post content, comments and post URLs from a site the administrator placed behind mandatory login.	3.7	More Details
CVE-2026-86421	ImageMagick before 7.1.2-30 and 6.9.13-55 contains a memory leak in the MSL image decoder. A crafted MSL image triggers memory allocation without proper deallocation, allowing an attacker to exhaust memory and cause a denial of service.	3.7	More Details
CVE-	A security flaw has been discovered in mwiede jsch up to 2.28.5. Affected is the function getRevokedKeys of the file src/main/java/com/jcraft/jsch/KnownHosts.java. Performing a manipulation of the argument known_hosts results in improper check for certificate revocation. The attack is possible to be carried out		

2026-86231	remotely. The attack is considered to have high complexity. The exploitability is told to be difficult. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.28.6 is able to address this issue. The patch is named 194a2f76a5c0f1c3f778565be3fd66bcafc42d23. You should upgrade the affected component.	3.7	More Details
CVE-2026-85008	undici's cache interceptor documents that only safe HTTP methods are cached, but its logic to skip caching is built by subtracting the configured methods from the set of safe methods, so an unsafe method such as POST, PUT, or DELETE is never placed in the skip list and instead falls through to the full cache-read path. The response-storage gate also lacked a method check, so a response to an unsafe request that is heuristically cacheable or carries an explicit Cache-Control directive is stored and later replayed from cache. Because response headers from a remote origin are untrusted, an origin can answer once with a cacheable status and then have the client's own subsequent state-changing requests to that path served from the stale cache entry without ever reaching the origin, an integrity failure that occurs under the interceptor's default configuration. This affects undici versions from 7.0.0 up to 7.29.1 and from 8.0.0 up to 8.10.2. Users should upgrade to undici 7.29.1 or 8.10.2.	3.7	More Details
CVE-2026-86301	A vulnerability has been found in code-projects Hospital Information System 1.0. Affected is an unknown function of the file /HIS/src/patients/editPatient.php of the component Patient Management. Such manipulation of the argument ID leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-76960	SAP S/4HANA Finance (Advanced Payment Management) does not perform sufficient Cross-Site Request Forgery protection on certain requests, due to this an attacker with low privileges could craft a malicious link or page. If an authenticated victim interacts with it, unintended actions could be triggered on the web server on their behalf. This results in a low impact on confidentiality and integrity. There is no impact on availability.	3.5	More Details
CVE-2026-85207	A vulnerability was identified in itsourcecode Online Medicine Delivery System 1.0. Impacted is an unknown function of the file /index.php?q=orderdetails. Such manipulation of the argument location leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used.	3.5	More Details
CVE-2026-78600	Incomplete Cleanup (CWE-459) in Elastic Cloud on Kubernetes (ECK) can lead to unauthorized access via Privilege Abuse (CAPEC-122). Authentication credentials persist after a cross-namespace association has been denied by RBAC enforcement, allowing a low-privileged tenant to retain unauthorized read access to the associated Elasticsearch cluster.	3.5	More Details
CVE-2026-84653	Jenkins 2.421 through 2.579 (both inclusive), LTS 2.426.1 through 2.568.2 (both inclusive) does not correctly perform permission checks in the Appearance configuration page, allowing attackers with Overall/Manage permission to modify Appearance configuration options they should not have access to.	3.5	More Details
CVE-2025-15692	The Icegram Express WordPress plugin before 5.8.6 does not properly escape a list description setting before outputting it within an HTML attribute, which could allow users with the Administrator role and above to perform Stored Cross-Site Scripting attacks.	3.5	More Details
CVE-2026-33920	A cross-site request forgery vulnerability was discovered in the login functionality (both standard and SAML) due to missing validation of the anti-CSRF token. An attacker with a valid account can trick a victim into unknowingly authenticating with the attacker's credentials. Any operation performed by the victim in this state is attributed to the attacker's account, compromising the integrity of the audit trail.	3.5	More Details
CVE-2025-15694	The Joli Table Of Contents WordPress plugin before 2.8.1 does not sanitise and escape some of its settings before outputting them in an admin page, which could allow high-privilege users such as administrators to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed, for example in a multisite setup.	3.5	More Details
CVE-2026-86226	A security flaw has been discovered in Projectwolds Online Attendance System 1.0. Affected by this issue is some unknown functionality of the file profile.php. The manipulation of the argument email results in cross site scripting. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	3.5	More Details
CVE-2025-52657	HCL MyXalytics was affected by Potential DOS Vulnerability. It allows users to input data without any restriction on the number of characters which can impact system performance or availability.	3.5	More Details
CVE-2026-76961	SAP S/4HANA Finance (Advanced Payment Management) does not perform sufficient Cross-Site Request Forgery protection on certain requests, due to this an attacker with low privileges could craft a malicious link or page. If an authenticated victim interacts with it, unintended actions could be triggered on the web server on their behalf. This results in a low impact on confidentiality and integrity. There is no impact on availability.	3.5	More Details
CVE-2025-52652	HCL MyXalytics was affected by Content Spoofing Vulnerability. It may allow an attacker to manipulate displayed content, making it appear as though it originates from a trusted source, potentially leading to phishing or data theft.	3.5	More Details
	A vulnerability was determined in OpenCart 4.1.0.3/4.1.0.4. This affects an unknown function of the file		

CVE-2026-84438	catalog/controller/account/edit.php of the component Autocomplete Workflow. This manipulation of the argument firstname causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-85405	A flaw has been found in Eleveo Call Recording Software 9.7.0. This affects an unknown part of the file /callrec/roleAddAction.do. Executing a manipulation of the argument name/username can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-86181	A vulnerability was found in code-projects Task Management System 1.0. Affected by this issue is some unknown functionality of the file /user/UpdateUserProfile.php of the component User Profile Update. The manipulation of the argument lname results in cross site scripting. The attack can be launched remotely. The exploit has been made public and could be used.	3.5	More Details
CVE-2026-86644	A vulnerability was determined in star7th showdoc up to 3.9.1. This vulnerability affects unknown code of the file web_src/public/editor.md/editormd.js of the component API Page Save Endpoint. Executing a manipulation can lead to cross site scripting. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 3.9.2 is able to resolve this issue. This patch is called a8ea1520850b4242f395247f72e87e597506cef0. Upgrading the affected component is recommended. The vendor confirms: "The fix [...] sets Mermaid `securityLevel` to `strict`, disables `htmlLabels`, and sanitizes rendered SVG with DOMPurify."	3.5	More Details
CVE-2026-85406	A vulnerability has been found in Eleveo Quality Management 9.7.0. This vulnerability affects unknown code of the component Conversation Review. The manipulation leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-19698	The GutenKit WordPress plugin before 2.5.1 does not validate or escape style settings saved against a post before using them to build the CSS it outputs on the front end, allowing users with the Contributor role and above to inject arbitrary CSS into pages served to other users and to anonymous visitors. JavaScript execution is not possible at that role, so the impact is limited to defacement, interface redressing and forcing external resources to load.	3.5	More Details
CVE-2026-84437	A vulnerability was found in OpenCart 4.1.0.3/4.1.0.4. The impacted element is an unknown function of the file catalog/controller/account/address.php of the component Autocomplete Workflow. The manipulation of the argument address_1 results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-52651	HCL MyXalytics was affected by Improper Input validation Vulnerability. It allow malicious or unexpected data to cause unintended system behaviour or security issues.	3.5	More Details
CVE-2026-85022	A vulnerability was identified in langgenius dify 1.13.0. Affected by this vulnerability is the function router.replace of the file web/app/(shareLayout)/webapp-signin/components/mail-and-password-auth.tsx of the component WebApp Sign-In. Such manipulation of the argument redirect_url leads to cross site scripting. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-86491	In JetBrains YouTrack before 2026.2.18634 stored XSS was possible via project and organization icon uploads	3.5	More Details
CVE-2026-81161	Privilege Defined With Unsafe Actions vulnerability in Drupal Content Moderation Notifications allows Privilege Escalation. This issue affects Content Moderation Notifications versions: from 0.0.0 to 3.9.0.	3.3	More Details
CVE-2026-86425	ImageMagick before 7.1.2-30 and 6.9.x before 6.9.13-55 contains a heap-use-after-free vulnerability in the Layer method of PerlMagick. An attacker who supplies a crafted list of images can trigger memory access after deallocation, resulting in a crash (denial of service).	3.3	More Details
CVE-2026-86505	In JetBrains IntelliJ IDEA before 2026.2.2 missing project-trust check leaked project metadata to JetBrains Marketplace	3.3	More Details
CVE-2026-86503	In JetBrains IntelliJ IDEA before 2026.2.2 opening an untrusted project could trigger SSRF via Kubernetes spec-source URL fetching	3.3	More Details
CVE-2026-86422	ImageMagick before 7.1.2-30 contains a time-of-check-time-of-use vulnerability in path policy enforcement on Windows that allows attackers to bypass read or write restrictions by exploiting symlink race conditions. Attackers can swap symlinks between policy validation and file access to read or write policy-denied files.	3.3	More Details

CVE-2026-86423	ImageMagick before 7.1.2-30 and 6.9.x before 6.9.13-55 contains a heap-use-after-free vulnerability in the GetList method of PerlMagick. A crafted call to the GetList method can trigger the use-after-free, resulting in a crash (denial of service).	3.3	More Details
CVE-2026-18858	IBM i 7.6, and 7.5 could allow a local authenticated attacker to obtain information from a privileged file when using SSH.	3.3	More Details
CVE-2021-48006	PocketMine-MP before 4.0.3 does not perform case-insensitive matching when removing operator entries from ops.txt. The removeOp function lowercases the supplied name but only removes an exactly matching entry, so an operator name stored with non-lowercase letters cannot be revoked using the deop command, leaving the player as an operator until the entry is removed from ops.txt manually.	3.3	More Details
CVE-2026-86485	In JetBrains YouTrack before 2026.2.18634 iP spoofing via HTTP headers allowed forged Bitbucket webhooks	3.3	More Details
CVE-2025-15614	ugrep before 7.6.0 contains a heap buffer over-read vulnerability in the LZW decompressor when processing crafted .Z archive files. Attackers can supply malformed .Z files that cause the decompressor to read one byte past the allocated heap buffer, potentially crashing the process.	3.3	More Details
CVE-2023-3360	The Weaver Show Posts WordPress plugin before 1.8.1 unserialises the content of an imported file, which could lead to PHP object injections issues when a high privilege user import a malicious file and a suitable gadget chain is present on the blog.	3.3	More Details
CVE-2026-78587	Incorrect Authorization (CWE-863) in Fleet Server can lead to a denial of service of agent upload operations via Privilege Abuse (CAPEC-122). Fleet Server does not correctly verify session ownership during multi-part data upload operations, allowing any authenticated agent to interfere with the active upload sessions belonging to other enrolled agents.	3.1	More Details
CVE-2026-84355	Incorrect authorization in Navigation in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to bypass web origin policy via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-86227	A weakness has been identified in valkey-io valkey up to 9.0.5/9.1.1. This affects the function kvstoreGetHashtable of the file src/kvstore.c. This manipulation of the argument didx causes out-of-bounds read. It is possible to initiate the attack remotely. The attack is considered to have high complexity. It is indicated that the exploitability is difficult. The exploit has been made available to the public and could be used for attacks. Patch name: 4691888e7fab3df128f0bde5750c9fde2ae552fa. To fix this issue, it is recommended to deploy a patch. Exploitation requires cluster mode plus attacker-controlled dump.rdb at startup (data-dir write access, replication feed, or a stored crafted RDB) - an attacker-position DoS at boot, not network pre-auth. The issue report was closed stating it "is worth fixing for the sake of memory safety… but I don't think it meets our bar for a security disclosure."	3.1	More Details
CVE-2026-84359	Information leak in Skia in Google Chrome prior to 152.0.7977.75 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-2026-84066	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9 does not verify that the requesting user owns the post being modified before writing uploaded file references to its metadata, allowing users with the subscriber role and above to overwrite image metadata on posts belonging to other users.	3.1	More Details
CVE-2026-85052	Out of bounds read in CrashReporting in Google Chrome prior to 152.0.7977.82 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-84331	Incorrect authorization in Actor in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to bypass web origin policy via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2026-49456	Waku is the minimal React framework. Prior to version 1.0.0-beta.1, the unstable_redirect() helper exported from waku/router/server (packages/waku/src/router/define-router.tsx:156–161) accepts an arbitrary string and reflects it unchanged into the HTTP Location response header with no URL validation, scheme restriction, or path-only enforcement. Any application that passes user-controlled input to this helper — the natural pattern documented in the JSDoc and official fixtures — is vulnerable to open redirect attacks. An attacker who convinces a victim to click a crafted link can silently redirect the browser to an arbitrary external domain, enabling phishing, credential harvesting, and OAuth token theft. Additionally, scheme-relative URLs (//evil.example/) bypass naive https?://-only allow-list filters that developers might add as ad-hoc mitigations. This issue has been patched in version 1.0.0-beta.1.	3.1	More Details
CVE-	A url redirection to untrusted site ('open redirect') vulnerability in Fortinet FortiSIEM 7.5.0 through 7.5.1,		

2026-84389	FortiSIEM 7.4.1 through 7.4.2 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	3.1	More Details
CVE-2026-84328	Missing authorization in FileSystem in Google Chrome prior to 152.0.7977.75 allowed a remote attacker who had compromised the renderer process to bypass web origin policy via a crafted HTML page. (Chromium security severity: Medium)	3.1	More Details
CVE-2026-63020	A vulnerability exists in an undisclosed BIG-IP Configuration utility page that may allow an attacker to spoof error messages Impact: An attacker may trick authenticated BIG-IP users into accessing malicious links and reflect a spoofed error message in the victim's BIG-IP Configuration utility web browser session. This is a control plane issue; there is no data plane exposure. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	3.1	More Details
CVE-2026-86487	In JetBrains YouTrack before 2026.2.18634 a crafted WebSocket message allowed read-only whiteboard users to modify canvas content	3.1	More Details
CVE-2026-86141	xmlregexp in libxml2 before 2.15.4 has a NULL pointer dereference in xmlRegNewParserCtxt after a strdup failure, i.e., it does not calculate a string length after NULL checking.	2.9	More Details
CVE-2026-86137	In libxml2 before 2.15.4, xmlFAParsePosCharGroup has an out-of-bounds read, aka an out-of-bounds read in the NXT macro in xmlregexp.	2.9	More Details
CVE-2026-86501	In JetBrains IntelliJ IDEA before 2026.2.2 terminal command input could be written to idea.log	2.8	More Details
CVE-2026-84392	A NULL Pointer Dereference vulnerability [CWE-476] vulnerability in Fortinet FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiPAM 1.9.0, FortiPAM 1.8 all versions, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.6.0 through 7.6.6, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an authenticated attacker to crash the httpsd daemon via crafted HTTP requests.	2.7	More Details
CVE-2026-73317	XenForo before 2.3.13 contains a missing authorization vulnerability in the ACP cache-rebuild dispatcher that allows limited administrators with only the rebuildCache permission to perform unauthorized approval queue actions by supplying an arbitrary job class and actor user ID in the POST body. Attackers can invoke the approval queue job under any user identity to approve queued user registrations without holding the required approval-queue or moderator permissions, causing the moderation log to attribute actions to an impersonated account.	2.7	More Details
CVE-2026-84927	The EmbedPress WordPress plugin before 4.6.4 does not perform a sufficient authorization check on one of its Google Reviews REST API routes, allowing users with the Contributor role and above to modify a site-wide store, deleting entries an administrator configured and injecting their own, which are rendered publicly across the site.	2.7	More Details
CVE-2026-82069	A security issue in MongoDB Server's query statistics serialization on the router allows users with monitoring privileges to access unredacted search query text from other users' operations. An improper conditional check in the serialization logic causes the data redaction mechanism to be bypassed when processing search queries through the sharded cluster router. This results in sensitive query literals being stored and made accessible through the query statistics interface.	2.7	More Details
CVE-2026-77784	The Rank Math SEO WordPress plugin before 1.0.277 does not verify that a user is allowed to edit the object being modified before updating its SEO indexing metadata, allowing users with the Author role and above to alter that metadata on content, taxonomy terms and user profiles they do not own, and to remove other users' content from the site's sitemap and search engine index.	2.7	More Details
CVE-2026-84926	The EmbedPress WordPress plugin before 4.6.4 does not correctly restrict access to one of its Google Reviews REST routes to administrators, allowing any authenticated user with contributor-level access or above to read the site administrator's email address, a value WordPress core withholds from that role.	2.7	More Details
CVE-2026-77787	The Rank Math SEO WordPress plugin before 1.0.277 does not perform a capability check when bulk metadata updates target taxonomy terms, and reuses the supplied object identifier across object types, allowing users with the Author role and above to modify the SEO metadata of terms they cannot edit and to overwrite the titles of posts belonging to other users.	2.7	More Details
CVE-2026-77785	The Rank Math SEO WordPress plugin before 1.0.277 does not verify that the requesting user is permitted to read the specific post referenced in a request before returning its content and SEO metadata, allowing users with the Author role and above to read the title, body and metadata of other users' non-public posts.	2.7	More Details

CVE-2026-81196	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.46 does not properly verify ownership of quiz question identifiers, allowing users with instructor access to read other instructors' quiz questions, including the correct answers and explanations.	2.7	More Details
CVE-2025-15693	The JCH Optimize WordPress plugin before 5.0.1 does not properly restrict a directory path provided to one of its administrative image-browsing features to within the site, allowing high-privilege users, administrators on single-site and sub-site administrators on multisite, to enumerate directories and file names outside the web root.	2.7	More Details
CVE-2026-78150	The Smart Post WordPress plugin before 4.0.8 does not check the type, ownership or status of the post it is asked to duplicate, allowing users with contributor privileges and above to copy any private or password protected post into a draft of their own and read its content and metadata.	2.7	More Details
CVE-2026-84745	The Events Calendar WordPress plugin before 6.17.3.1 does not restrict non-public content to the users entitled to read it on its public REST archives, allowing users with a low-privilege role such as contributor to read the full contents of every unpublished record on the site, including other users'.	2.7	More Details
CVE-2026-45197	Kernel software installed and running inside a Guest VM may post improper commands to the GPU Firmware to trigger a read and/or write data outside the Guest's virtualised GPU memory. The firmware uses data provided by the Guest VM to set up accesses to memory. It validated this before use, but a TOCTOU bug was present which allowed the earlier check results to be invalidated.	2.5	More Details
CVE-2026-86424	ImageMagick before 7.1.2-30 and 6.9.13-55 contains a time-of-check-time-of-use (TOCTOU) vulnerability in the video decoder that allows attackers to bypass path policy write restrictions via symlink swaps. An attacker can replace a symlink between policy validation (check-time) and the file write operation (use-time) to write to policy-denied locations.	2.5	More Details
CVE-2026-58234	SAP Process Integration (SOAP Adapter) allows a privileged user to send specially crafted requests containing deeply nested entity definitions, which under certain conditions could temporarily increase processor load and degrade system responsiveness. Successful exploitation results in low impact on availability with no impact on confidentiality and integrity.	2.2	More Details
CVE-2026-84225	The Kirki WordPress plugin before 6.3.0 does not check that a user is allowed to act on a collaboration comment before changing its state, allowing users whom an administrator has granted content-level access to the page builder to modify comments left by other users, including on pages they cannot themselves open.	2.2	More Details
CVE-2026-23589	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-23590	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-7477	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform valid GPU memory processing operations to access already freed memory. This issue affects Bifrost GPU Kernel Driver: from r44p0 through r49p4, from r50p0 through r51p0, from r54p1 through r54p2; Valhall GPU Kernel Driver: from r44p0 through r49p5, from r50p0 through r54p3; Arm 5th Gen GPU Architecture Kernel Driver: from r44p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-84175	In Eclipse Ditto versions 3.0.0 to 3.9.6, the Things service fetches WoT (Web of Things) ThingModels over HTTP from URLs supplied by API users in the definition field of a Thing or Feature, without validating the target host, and follows HTTP redirects without re-validating the redirect target and without a hop limit. An authenticated user who is permitted to create a Thing, or who holds WRITE permission on an existing Thing, can thereby cause the Things service to issue arbitrary HTTP GET requests from inside the deployment's network — including to cloud instance-metadata endpoints and other internal services — and can use the differing error responses returned to the caller to enumerate internal services. Versions 2.4.0 to 2.5.x contain the same code, but are only affected where the operator explicitly enabled the WoT integration feature toggle, which is disabled by default in those versions.	N/A	More Details
CVE-2026-23591	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-11573	Uncontrolled recursion in Qt's QDomDocument serialization (QtXml) lets deeply nested untrusted XML crash the app via stack exhaustion (DoS only).	N/A	More Details
CVE-	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU memory processing operations to access already freed memory. This issue affects Bifrost GPU Kernel		More

2026-7476	Driver: from r49p3 through r49p5, r51p0, from r54p1 through r54p2; Valhall GPU Kernel Driver: from r49p3 through r49p5, from r51p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r49p3 through r49p5, from r51p0 through r54p3, r55p0.	N/A	Details
CVE-2026-79577	An issue in the /cas/login component of sso-master v1.0.0 allows attackers to authenticate into the application without a password via sending a crafted POST request.	N/A	More Details
CVE-2026-23587	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-79575	The JWT signing secret in yfexam-exam v2.0 is derived from the username and the current month instead of a random server-side key, making the secret key easily obtainable via a bruteforce attack.	N/A	More Details
CVE-2026-79571	Incorrect access control in the SellerAuthorizeAspect component of springboot-project v1.0.0 allows unauthenticated attackers to access all seller management interfaces and list all products/orders, put products on/off sale, finish/cancel orders, and modify categories without authentication.	N/A	More Details
CVE-2026-86426	LibreNMS before 26.8.0 contains an authentication bypass vulnerability in the REST API that allows unauthenticated attackers to access protected endpoints by sending numeric values instead of string tokens. Attackers can exploit MySQL type coercion by sending small integers like 0 through 9 to match token hashes, gaining access to API functionality including device credentials and administrative features that enable remote code execution through alert templates.	N/A	More Details
CVE-2026-86840	The `vtoken-minting` and `slpx` pallets in Bifrost contain an improper authorization vulnerability in channel commission attribution. A signed account can supply an arbitrary registered `channel_id` when minting tokens without verifying that the caller is authorized to mint on behalf of that channel. This allows an attacker to inflate a channel's recorded mint volume and cause protocol commission payments to be disproportionately distributed to that channel during commission settlement.	N/A	More Details
CVE-2026-78837	A SQL injection vulnerability in the ap_form_{id} parameter in AppNitro MachForm v30 allows attackers to access sensitive database information via a crafted SQL statement.	N/A	More Details
CVE-2026-70614	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-70613	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-5729	Use After Free vulnerability in Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform valid GPU processing operations to access already freed memory. This issue affects Valhall GPU Kernel Driver: from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-81638	Improper Handling of Alternate Encoding vulnerability in ash-project ash_double_entry allows an attacker to submit several distinct string spellings of the same identifier. AshDoubleEntry.ULID renders a 128-bit ULID as 26 Crockford base-32 characters, but the first character encodes only 3 bits, so canonical values are 0 to 7. decode/1 in lib/ulid.ex masks the first character to its low 3 bits and valid?/1 accepts all 32 characters in that position, so 0..., 8..., G... and R... decode to the identical 16-byte value and resolve to the same row. When the type is exposed as a public ID over an HTTP or API boundary, an attacker-supplied ID can be spelled differently from the record it actually reads or writes, desynchronizing or bypassing string-level checks such as idempotency and deduplication keys, deny-lists, audit correlation, or signatures computed over the submitted ID. This issue affects ash_double_entry: from 0.1.0 before 1.0.19.	N/A	More Details
CVE-2026-23588	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-52307	An authenticated stored cross-site scripting (XSS) vulnerability in the Column Management component of ClassCMS 1CMS v5.6 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the title field.	N/A	More Details
CVE-2026-	Affected versions of MISP insufficiently validate URLs used by dashboard widgets, particularly the Button widget. The widget's URL is stored configuration controlled by a user. The previous renderer considered a URL safe if it appeared relative or if its parsed hostname matched the configured MISP hostname. That logic failed to reject dangerous schemes and URL forms that browsers normalize differently from PHP's URL parsing. As a result, values such as javascript: URLs or backslash-based authority forms could reach the	N/A	More

86440	generated anchor's href and execute script or navigate to an attacker-controlled origin when another user interacted with the widget. The upstream commit describes the issue as: “javascript: and backslash URLs reached the href (stored XSS)”. The fix routes widget URLs through a shared DashboardURLValidator, rejects dangerous schemes, raw backslashes, control characters, and unauthorized absolute origins, and validates the URL both in the widget handler and renderer. Version affected: ≤2.5.45		Details
CVE-2026-79572	An XXE (XML External Entity) vulnerability in the level-rule module of Distribution Management v1.0.0 allows attackers to read sensitive files, scan internal networks, or launch server attacks via supplying a crafted XML payload.	N/A	More Details
CVE-2026-23586	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-23585	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-81531	An information disclosure vulnerability has been identified in Omada Controller. An API endpoint intended for Controller initialization remains accessible after completion and may disclose account-related information to unauthenticated remote users. Successful exploitation may allow an attacker to remote query the affected endpoint that may facilitate user enumeration and subsequent attacks targeting administrative accounts.	N/A	More Details
CVE-2026-79570	mfish-nocode-pro v1.0.0 was discovered to contain a SQL injection vulnerability in the tableName parameter at /sys/dbConnect/data. This vulnerability allows attackers to access sensitive database information via a crafted SQL statement.	N/A	More Details
CVE-2026-78997	UC Browser for Android (package com.UCMobile.intl, version 13.7.8.1314) contains a Universal Cross-Site Scripting vulnerability that allows an attacker to execute arbitrary JavaScript in the context of any origin. An attacker hosts a specially crafted URL on a UC-owned domain (via a reflected XSS) that leverages the browser's internal JavaScript bridge to register a deferred callback, navigate the tab to a victim site, and then execute attacker-controlled code on that site when a login dialog is dismissed.	N/A	More Details
CVE-2026-78230	AshAi exposes Ash read actions to language-model tool calls. The read tool accepts an aggregate result type (min, max, sum, avg) that builds an ad-hoc Ash.Query.Aggregate over a named field and returns its raw value. Ash field policies redact forbidden fields on returned records (replacing them with %Ash.ForbiddenField{}), but that redaction does not apply to aggregate values. A tool caller could therefore read a field the calling actor's field policies forbid by requesting it as an aggregate; min/max in particular return an actual field value. This includes fields that are public? true but restricted per-actor by a field policy, such as sensitive PII. The tool's existing check only required the field to be public, which is a separate axis from per-actor field-policy authorization. The fix authorizes the aggregated field against the resource's field policies, so aggregating over a field the actor may not see is refused or scoped to the rows where it is visible. This issue affects ash_ai: from 0.1.0 before 1.0.3.	N/A	More Details
CVE-2026-86452	Affected versions of MISP permit unauthenticated or weakly constrained request paths to perform persistent work without adequate input bounds or rate limiting. The users/forgot password-reset endpoint accepted an attacker-controlled email value without first imposing a reasonable length bound or validating its format. That value was then used to create an audit log entry and queue a password-reset job, causing the supplied value to be persisted more than once per request. The commit explicitly states that an unbounded unauthenticated request field was stored twice per call with no throttle. The fix adds: * a maximum email input length of 1024 bytes; * email-format validation before persistent work; * a per-source pre-authentication request budget; * HTTP 429 responses when that budget is exceeded; * a 15-minute cooldown for API-access request emails; * POST-only handling and CSRF protection for the API-access request endpoint. The new flood filter is specifically intended to limit persistent storage costs from anonymous requests such as password resets, registrations, and failed REST authentication attempts. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-79574	An issue in the gateway server of mpush v0.8.1 allows attackers to execute arbitrary code via sending a crafted broadcast message.	N/A	More Details
CVE-2026-23584	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-79573	L-ONE v1.0.0 was discovered to contain multiple SQL injection vulnerabilities in the /attachment/getBusinessUploadList component via the busid, id, and taskid parameters. This vulnerability allows attackers to access sensitive database information via a crafted SQL statement.	N/A	More Details
CVE-2026-86073	n8n is an open source workflow automation platform. Prior to 2.37.7 and 2.38.1, the OAuth token endpoint bound an authorization code's first access token to the consented resource but did not bind its refresh token. Refreshing checked only that the requested resource was registered, not that it matched the original grant. An OAuth client approved for one workflow could substitute a different workflow URL in the resource	N/A	More Details

	parameter and obtain a valid token for an unapproved workflow accessible to the consenting user. This issue is fixed in versions 2.37.7 and 2.38.1.		
CVE-2026-86441	Affected versions of MISP contain inconsistent authorization checks across dashboard widgets that display organisation information. Several organisation-related widgets did not honor Security.hide_organisation_index_from_users. As a result, authenticated users without the perm_sharing_group permission could enumerate organisations even though the normal organisation index was intentionally hidden from them. The affected widgets included paths that: * returned organisation names and identifiers; * could expose additional organisation database fields through JSON export because unrestricted find('all') queries fetched full rows; * accepted limit=0 or negative values in a way that could effectively remove the result limit and return the entire organisation table. A related organisation-contributor leaderboard also ignored the same visibility setting. Its handler counted Event.orgc_id across the entire event table and mapped those IDs to organisation names, revealing every organisation with events regardless of whether the caller could see any of those events. The fix withdraws this widget entirely for users who lack organisation-index visibility. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-16769	An unencrypted 'pause encryption request' message causes a denial of service in the in the RS9116W/SiWx917. See vulnerability B-E10 in the related paper below.	N/A	More Details
CVE-2026-9040	A race condition vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU memory processing operations to cause a denial of service or disclose sensitive information. This issue affects Bifrost GPU Kernel Driver: from r12p0 through r49p5, from r50p0 through r51p0, from r54p1 through r54p2; Valhall GPU Kernel Driver: from r19p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-9034	Use After Free vulnerability in Arm Ltd Bifrost GPU Userspace Driver, Arm Ltd Valhall GPU Userspace Driver, Arm Ltd Arm 5th Gen GPU Architecture Userspace Driver allows a non-privileged user process to perform valid GPU processing operations, including via WebGL or WebGPU, to access already freed memory. This issue affects Bifrost GPU Userspace Driver: from r42p0 through r49p5, from r50p0 through r51p0, from r54p1 through r54p3; Valhall GPU Userspace Driver: from r42p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Userspace Driver: from r42p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-78216	AshLua exposes Ash read actions to Lua scripts run through an eval action. A read call accepts an operation (list, min, max, first, sum, avg) that builds an ad-hoc Ash.Query.Aggregate over a named field and returns its raw value. Ash field policies redact forbidden fields on returned records (replacing them with %Ash.ForbiddenField{}), but that redaction does not apply to aggregate values. A script could therefore read a field the calling actor's field policies forbid by requesting it as an aggregate instead of as a field. This includes fields that are public? true but restricted per-actor by a field policy, such as sensitive PII. The prior hardening only enforced the exposed-field allow-list (field visibility), which is a separate axis from per-actor field-policy authorization. The fix authorizes the aggregated field against the resource's field policies, so aggregating over a field the actor may not see is refused or scoped to the rows where it is visible. This issue affects ash_lua: from 0.1.0 before 0.2.2.	N/A	More Details
CVE-2026-82958	In Eclipse Ditto versions [1.3.0, 3.9.6], the ImplicitThingCreationMessageMapper of the connectivity service builds a CreateThing command by substituting placeholder values (e.g. {{ header:device_id }}) resolved from inbound message headers into a pre-configured JSON "thing" template as raw, un-escaped strings, and then parses the resulting string as JSON. Because the placeholder engine performs no JSON escaping and is unaware of the surrounding JSON string context, a resolved value containing a double-quote character can break out of its string and inject additional JSON structure. When a connection is configured to use this mapper with a template that reflects a header whose value a publishing device can control (for example an MQTT 5 user property, an AMQP 1.0 application property, or a Kafka record header), an attacker able to publish on that connection can inject an inline _policy object. The inline policy overrides the administrator-configured policyId, letting the attacker assign an arbitrary access-control policy to the newly created digital twin — gaining full read/write access to it and potentially revoking the legitimate owner's access, with no administrator interaction. Exploitation requires all of the following: the connection uses the (non-default) ImplicitThingCreation mapper; its template reflects an attacker-controllable header; and, for the policy-override impact, the connection's authorization subjects are permitted to create policies (the default). Deployments that restrict the connection's subjects to thing creation only via the entity-creation configuration are not affected by the policy-override impact.	N/A	More Details
CVE-2026-86135	A Cross-Site Request Forgery (CSRF) vulnerability in WatchGuard Dimension's database snapshot creation feature allows a remote attacker to trigger unauthorized snapshot creation by tricking an authenticated administrator into visiting a specially crafted web page.	N/A	More Details
CVE-	A Server-Side Request Forgery (SSRF) vulnerability exists in the ONLYOFFICE ownCloud Integration plugin version 9.12. The /apps/onlyoffice/ajax/settings/address endpoint does not sufficiently validate the user-supplied Document Server URL before initiating outbound connections. An authenticated administrator can		More

2026-84282	manipulate the document server parameter to cause the ownCloud server to send arbitrary requests to attacker-controlled destinations, including localhost and internal network hosts. This allows internal network reconnaissance and TCP port scanning based on differences in server responses.	N/A	Details
CVE-2026-23583	Rejected reason: Withdrawn by requester.	N/A	More Details
CVE-2026-33197	AMI APTIOV contains a vulnerability in BIOS where a privileged user may cause the “Incomplete List of Disallowed Inputs” by local access. Successful exploitation of this vulnerability may lead to arbitrary code execution and impact system Confidentiality, Integrity, and Availability.	N/A	More Details
CVE-2026-86451	Affected versions of MISP allow authenticated users to retrieve object-reference records by UUID through EventGraphTool::get_reference_data() without first checking whether the requester is authorized to view the object the reference belongs to. The vulnerable code queried ObjectReference.uuid directly and returned the matching row whenever it existed. Because no parent-object ACL was applied, a user who knew or obtained a reference UUID could retrieve information associated with an object outside their normal access scope. The commit explicitly states that any object reference could be returned by UUID without authorizing its parent object. The fix retrieves the referenced object's object_id and calls fetchObjectSimple() with the current user. If the user cannot access that parent object, MISP now returns NotFoundException instead of exposing the reference. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-86408	Affected versions of MISP do not enforce parent-event visibility when serving cryptographic keys through CryptographicKeysController::view(). The vulnerable handler queried CryptographicKey directly using the supplied key ID and selected sensitive fields such as: * type * key_data * fingerprint but did not fetch or authorize the associated parent event first. The upstream commit explicitly states that cryptographicKeys/view could return a protected event’s signing key to any authenticated user. The fix adds parent_id and parent_type to the lookup and then enforces authorization through the associated event using fetchSimpleEvent($user, parent_id). If the parent is not an Event, access is limited to site administrators. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-86419	Affected versions of MISP contain insufficient validation of server-side outbound HTTP destinations in feed retrieval and TAXII discovery functionality. In feed processing, redirects were followed without validating the redirect scheme or destination. The original request headers were reused across redirect hops, meaning authentication headers or API credentials configured for a feed could be forwarded to a different host. Redirects could also target internal network resources, resulting in SSRF. The fix adds redirect validation, blocks internal destinations for cross-host redirects, strips configured feed credentials before following redirects to another host, and pins validated DNS results to prevent re-resolution after validation. The TAXII discovery endpoint had a related incomplete SSRF defense. It used gethostbyname() and compared the result against only a few literal addresses. This missed cases including IPv6 loopback (::1), numeric host encodings such as 0x7f000001, and potentially multiple DNS records. The fix moves TAXII discovery to the shared URL egress validator. Together, these commits harden MISP's outbound URL handling against alternate-address representations, DNS-related bypasses, unsafe redirects, internal-host access, and cross-host credential forwarding. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-86417	Affected versions of MISP inconsistently enforced email-address visibility in DashboardsController::listTemplates(). The query always fetched User.email, while redaction happened only inside the non-REST rendering branch. As a result, the same authenticated user who saw redacted data in the normal HTML interface could request the REST/JSON representation and receive template owners’ email addresses without the intended privilege check. The fix moves the decision to a centralized User::canSeeEmails() authorization helper. Email addresses are now fetched only when the requester is a site administrator or the instance explicitly enables Security.disclose_user_emails. The same helper is also reused by other dashboard widgets to keep email-disclosure policy consistent. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-77104	CommServe contained a path traversal issue affecting information disclosure. Software customers upgrade to resolved maintenance release. Update CommServe.	N/A	More Details
CVE-2026-75810	Exposed Dangerous Method or Function in ASUS Armoury Crate allow a local user to cause a brief system stall by bypassing driver authentication and sending requests to trigger system management interrupts (SMIs). Repeatedly triggering SMI may lead to a denial-of-service (DoS) condition.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-19754	Baserow 2.3.3 contains a SQL injection vulnerability in the index() formula function. A low-privileged authenticated user who can create or modify formula fields can provide an undocumented fourth argument that is treated as a SQL template and interpolated directly into a PostgreSQL expression. The vulnerable expression is executed when Baserow recalculates formula field values. Because the generated SQL runs through Baserow's database connection, the injected SQL executes with the privileges of the Baserow PostgreSQL role rather than the permissions of the authenticated application user. This issue affects Baserow: 2.3.3.	N/A	More Details

CVE-2026-75811	Improper Restriction of Software Interfaces to Hardware Features in ASUS Armoury Crate allows a local user to modify hardware configuration settings and potentially cause hardware damage by bypassing driver authentication and accessing critical model-specific registers.Refer to the ' Security Update for Armoury Crate App' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-77132	It has been discovered that several AJAX routes used for the backend localization wizard failed to perform authorization checks. This allowed authenticated, low-privileged backend users to access information about records and content elements that fall outside of their permitted range. Exploiting this vulnerability requires a low-privileged backend user account. This issue affects TYPO3 CMS versions 10.0.0-10.4.59, 11.0.0-11.5.53, 12.0.0-12.4.48, 13.0.0-13.4.34 and 14.0.0-14.3.6.	N/A	More Details
CVE-2026-85400	Backend administrators without system maintainer privileges were able to schedule any of the configuration:read, configuration:set, and configuration:show commands. This allowed them to modify arbitrary system configuration, which is normally limited to system maintainers. As a consequence, this allowed them, for example, to gain system maintainer privileges or cause a denial of service. Exploiting this vulnerability requires an administrator-level backend user account. This issue affects TYPO3 CMS versions 14.2.0-14.3.6.	N/A	More Details
CVE-2026-86590	In Eclipse Che versions 7.79.0 through 7.121.0, the dashboard backend's POST /dashboard/api/data/resolver endpoint passes a caller-supplied URL directly to an outbound HTTP GET request with no host filtering. An authenticated user can exploit this server-side request forgery (SSRF) to read responses from internal network addresses, including the cloud instance metadata service (169.254.169.254), loopback interfaces, RFC-1918 private ranges, and in-cluster Kubernetes services. The operator-configured allowlist (spec.devEnvironments.allowedSources.urls) is not consulted. The vulnerability is fixed in version 7.122.0, which adds private-address blocking, IPv4-mapped IPv6 bypass prevention, operator allowlist enforcement, and disables HTTP redirects on the outbound request.	N/A	More Details
CVE-2026-19614	The API is prone to XML external entity (XXE) injection. By default, XML external entity support is enabled. This issue affects NanoXML: 2.2.3.	N/A	More Details
CVE-2026-79602	A guest with a PCI device assigned that has at least a BAR on the IO port space can trigger a BUG() in Xen.	N/A	More Details
CVE-2026-77106	Cvlaunchd contained a missing authorization issue affecting command execution authorization. Software customers upgrade to resolved maintenance release. Update all Commvault installations, including Commserve, Webserver, Command Center, Media Agents, Clients and HyperScale X.	N/A	More Details
CVE-2026-77105	CommServe contained a cryptographic signature verification issue affecting privilege management. Software customers upgrade to resolved maintenance release. Update CommServe and Web Server.	N/A	More Details
CVE-2026-77103	CommServe contained an authentication bypass issue affecting access authorization and information disclosure. Software customers upgrade to resolved maintenance release. Update CommServe.	N/A	More Details
CVE-2026-75808	Allocation of Resources Without Limits or Throttling in ASUS Armoury Crate allows a local user to cause a denial-of-service condition through system memory exhaustion by bypassing driver authentication and allocating an unrestricted amount of memory.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-77102	CommServe contained a heap-based buffer overflow issue affecting service availability. Software customers upgrade to resolved maintenance release. Update CommServe.	N/A	More Details
CVE-2026-77101	CommServe contained a stack-based buffer overflow issue affecting service availability. Software customers upgrade to resolved maintenance release. Update CommServe.	N/A	More Details
CVE-2026-77098	Private Metrics Server contained an SQL injection condition affecting database operations. Software customers upgrade to resolved maintenance release. Update Private Metrics Server.	N/A	More Details
CVE-2026-77097	Private Metrics Server contained a missing authentication condition affecting metrics upload functionality and service availability. Software customers upgrade to resolved maintenance release. Update Private Metrics Server.	N/A	More Details
CVE-2026-77654	Improper Privilege Management vulnerability in Horizon Security Analyzer (formerly AlgoSec Firewall Analyzer) on Linux, 64 bit allows Privilege Escalation and Parameter Injection. A local user with access to the command line may escalate their privileges by abusing the parameters of a command that is approved in the sudoers file. This issue affects Horizon Security Analyzer : A33.10, A33.20 and A33.30.	N/A	More Details

CVE-2026-77092	Content Extractor contained a deserialization of untrusted data issue affecting privilege management. Software customers upgrade to resolved maintenance release. Update Content Extractor.	N/A	More Details
CVE-2026-77091	DataCube contained a path traversal issue affecting security feature enforcement. Software customers upgrade to resolved maintenance release. Update Content Extractor and Index Store.	N/A	More Details
CVE-2026-77089	Command Center API contained an authentication bypass issue affecting privilege management. Software customers upgrade to resolved maintenance release. Update Command Center.	N/A	More Details
CVE-2026-62437	When guests are terminated, various pieces of cleanup need carrying out. The cleaning up of PCI devices which were assigned to guests, and the associated removal of tracking structures for IRQs used by the devices occurs relatively early in the process. Unfortunately after that point the guest about to be terminated could cause its device model (DM) to re-establish such tracking structures, by having it bind one or more IRQs anew. While some of those tracking structures would still be cleaned up later on, at least one would not be.	N/A	More Details
CVE-2026-19203	A client may issue specially crafted HTTP/1.1 chunked requests to a Jetty server that cause Jetty and an intermediary proxy to interpret different request boundaries, potentially resulting in HTTP request smuggling. This is caused by Jetty accepting a lone LF character as a terminator in parts of chunked request parsing. Depending on the Jetty version and configured HTTP compliance mode, this may occur in chunk extensions, chunk data termination, or trailer termination.	N/A	More Details
CVE-2026-75809	Exposed IOCTL with insufficient access control in ASUS Armoury Crate allows a local user to disclosure information and disabling device functionality by bypassing driver authentication and using IOCTLs to read from and write to PCIe configuration space.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-19397	Missing authentication for a critical function in ASUS Control Center Express Agent allows an unauthenticated nearby user to control the host via a direct connection to the agent when the host has an active login session. Refer to the ' Security Update for ASUS Control Center Express Agent ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-86418	Affected versions of MISP expose organisation metadata through the dashboard organisation picker without applying the same visibility restrictions enforced by the normal organisation index and per-organisation view. The affected endpoint returned fields including: * organisation ID; * UUID; * name. When Security.hide_organisation_index_from_users was enabled, normal organisation enumeration was restricted, but the dashboard picker still queried all organisations. This allowed authenticated users to discover organisations that should have remained hidden from them. The fix calls Organisation::createConditions($this->Auth->user()) and appends the resulting ACL conditions to the picker query. Ordinary users are thereby limited to organisations associated with events or proposals they can already see, plus their own organisation, while users with the appropriate sharing-group privilege retain broader visibility. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-79379	A buffer overflow in the SBC_DecodeFrames() function of Bestechnic Co., Ltd BES2300 Bluetooth Audio SoC firmware v3.x and earlier and fixed in v.5.0 allows attackers to cause a Denial of Service (DoS) via sending a crafted frame.	N/A	More Details
CVE-2026-82586	Improper Protection of Alternate Path vulnerability in ash-project ash_lua allows a user-supplied Lua script to read attributes that are not on the exposed-field allow-list. AshLua exposes Ash resources to Lua scripts, gated by a manifest declaring which fields are exposed. The read action's operation aggregate path in AshLua.Runtime took the field name straight from the Lua call and resolved it with only String.to_existing_atom and Ash.Query.Aggregate.new!, neither of which consults the exposed-field allow-list the normal fields path enforces. A script can therefore read the value of any attribute of any record the actor may read, including private sensitive?: true columns, via resource.read({ operation = {"list", "hashed_password"} }); min and max give a value oracle. Anyone able to submit or influence a Lua script can reach this. This issue affects ash_lua: from 0.1.0 before 0.2.1.	N/A	More Details
CVE-2026-12611	A client may issue HTTP/2 requests to a Jetty server that result in blocking writes that are never unblocked, eventually causing all threads to be blocked and the whole server to become unresponsive. This is caused by a race condition in the server when handling RST_STREAM frames and GOAWAY frames sent by the client. The race condition "resets" the HTTP2Flusher.terminated, previously set to a non-null value, to the null value, allowing entries to be enqueued in the flusher that however will never be processed. These unprocessed entries are the ones that would unblock the write-blocked threads.	N/A	More Details
CVE-2026-	Allocation of Resources Without Limits or Throttling vulnerability in ash-project ash_authentication_oauth2_server allows an unauthenticated attacker to exhaust database storage and memory. The /authorize endpoint is unauthenticated by design. With Client ID Metadata Documents enabled, resolve_client/3 in AshAuthentication.Oauth2Server.CIMD fetches the document for each new URL-shaped client_id and upserts a client row, with no cap on the number of rows, no expiry or garbage collection, and no	N/A	More

82753	length bound on the fetched fields; the document was also placed in CIMD.Cache before validation, so even rejected documents held cache memory until their TTL. An attacker serving valid documents at many distinct URLs creates one permanent client row per URL, each able to carry multi-megabyte strings, growing storage and memory without bound. This issue affects ash_authentication_oauth2_server: from 0.3.0 before 0.3.1.		Details
CVE-2026-12387	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform valid GPU memory processing operations to access already freed memory. This issue affects Bifrost GPU Kernel Driver: from r41p0 through r49p5, from r50p0 through r51p0, from r54p1 through r54p2; Valhall GPU Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-12285	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform valid GPU memory processing operations to access already freed memory. This issue affects Bifrost GPU Kernel Driver: from r41p0 through r49p5, from r50p0 through r51p0, from r54p1 through r54p2; Valhall GPU Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-11891	Use After Free vulnerability in Arm Ltd Valhall GPU Userspace Driver, Arm Ltd Arm 5th Gen GPU Architecture Userspace Driver allows a non-privileged user process to perform valid GPU processing operations, including via WebGL or WebGPU, to access already freed memory. This issue affects Valhall GPU Userspace Driver: from r46p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Userspace Driver: from r46p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-82754	Improper Protection of Alternate Path vulnerability in ash-project ash_authentication_oauth2_server exposes the state-changing OAuth endpoints under an unintended URL prefix, bypassing controls scoped to the canonical prefix. oauth2_server_protocol_routes/1 in AshAuthentication.Phoenix.Oauth2Server.Router forwards the same ProtocolRouter at both the /oauth prefix and the /.well-known prefix. Phoenix forward strips the matched prefix before dispatch, so the full route table answers under both mounts, and POST /register, POST /token, and POST /revoke are reachable as /.well-known/register, /.well-known/token, and /.well-known/revoke. Edge controls such as WAF rules, rate limits, or authentication exemptions written against the /oauth paths, or that allow-list /.well-known as unauthenticated, do not apply to the alias. This issue affects ash_authentication_oauth2_server: from 0.1.0 before 0.3.1.	N/A	More Details
CVE-2026-82755	Use of Cache Containing Sensitive Information vulnerability in ash-project ash_authentication_oauth2_server allows a shared HTTP cache to serve one tenant's OAuth discovery metadata to another tenant's clients. The RFC 8414 and RFC 9728 metadata endpoints in AshAuthentication.Phoenix.Oauth2Server.ProtocolRouter return tenant-specific values (issuer, authorization_endpoint, token_endpoint, jwks_uri) when a tenant is set, but sent them with Cache-Control: public, max-age=3600 and no Vary. When the tenant is derived from something other than the URL (a header or the Host) and a shared cache sits in front, the cache key is the URL alone, so a stored response for one tenant is served to another for up to an hour. Affected clients may then send authorization codes and secrets to the wrong tenant's token endpoint and validate tokens against the wrong keys. This issue affects ash_authentication_oauth2_server: from 0.1.3 before 0.3.1.	N/A	More Details
CVE-2026-82756	Improper Encoding or Escaping of Output vulnerability in ash-project ash_authentication_oauth2_server allows an unauthenticated attacker to inject arbitrary authentication parameters into the WWW-Authenticate challenge header. BearerPlug and RequireScopePlug built the Bearer resource_metadata="..." challenge by interpolating a resource_metadata URL derived from the request tenant directly into the quoted value. In a multi-tenant application that sets the Ash tenant from request-controlled data (a subdomain, the Host, a path segment, or a header), a tenant containing a " closes the quoted value and appends attacker-chosen auth-params, including a second resource_metadata URL pointing at an attacker-controlled authorization server that spec-following clients follow. Carriage returns and line feeds are rejected by Plug, so this is parameter injection within one header, not response splitting. This issue affects ash_authentication_oauth2_server: from 0.1.3 before 0.3.1.	N/A	More Details
CVE-2026-0860	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Arm Ltd Valhall GPU Kernel Driver, Arm Ltd Arm 5th Gen GPU Architecture Kernel Driver allows a local non-privileged user process to perform improper GPU memory processing operations to gain access to sensitive kernel information. This issue affects Valhall GPU Kernel Driver: from r29p0 through r49p5, from r50p0 through r54p3, r55p0; Arm 5th Gen GPU Architecture Kernel Driver: from r41p0 through r49p5, from r50p0 through r54p3, r55p0.	N/A	More Details
CVE-2026-79378	An issue in the btm_acl_handle() function of Bestechnic Co., Ltd BES2300 Bluetooth Audio SoC firmware v3.x and earlier allows attackers to cause a Denial of Service (DoS) via sending a crafted L2CAP packet.	N/A	More Details
CVE-2026-18023	Sensitive Information in Resource Not Removed Before Reuse in ASUS Armoury Crate driver allows a local user to disclose sensitive information from uninitialized memory via a crafted IOCTL request that bypasses the driver's security verification mechanism. Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
	Server-Side Request Forgery (SSRF) vulnerability in ash-project ash_authentication_oauth2_server allows an		

CVE-2026-82757	attacker who controls a client metadata URL and its DNS to make the server connect to internal or loopback addresses. public_ip?/1 in AshAuthentication.Oauth2Server.CIMD.ReqFetcher enforces the outbound policy for CIMD metadata fetches. It classified several address forms as publicly routable that are not: IPv4-compatible ::/96 (for example ::127.0.0.1), SIIT IPv4-translated ::ffff:0:0:0/96, and deprecated site-local fec0::/10. A returned AAAA record in one of these ranges passed the policy, so a fetch pinned to that address reached space the policy was meant to block. This issue affects ash_authentication_oauth2_server: from 0.3.0 before 0.3.1.	N/A	More Details
CVE-2026-78838	A reflected cross-site scripting (XSS) vulnerability in the grid_datasource.php component of AppNitro MachForm v30 allows attackers to execute arbitrary Javascript in the context of the victim's browser via injecting a crafted payload into the filter[filters][0][field] parameter.	N/A	More Details
CVE-2026-82758	Improper Authentication vulnerability in ash-project ash_authentication_oauth2_server allows an unauthenticated attacker to register OAuth clients even when Dynamic Client Registration is gated by an initial access token. resolve_secret/3 in AshAuthentication.Oauth2Server (reached through __resolve_secret__!) treated any return other than {:ok, _} or :error from a configured {module, function, args} or 2-arity-function secret provider as a valid secret, wrapping nil, false, or "" as {:ok, value}. When the initial_access_token resolves to such an empty value, POST /oauth/register compares the presented bearer token against it and the comparison passes with no token supplied, so registration is open although it was configured closed. The same fail-open affected other resolved secrets such as signing_secret. This issue affects ash_authentication_oauth2_server: from 0.1.0 before 0.3.1.	N/A	More Details
CVE-2026-82710	Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in ash-project usage_rules allows a malicious package publisher to inject terminal control sequences into the output of mix usage_rules.search_docs. mix usage_rules.search_docs searches Hex documentation through search.hexdocs.pm, which indexes the documentation of every published package, and prints the matching results (title, package, type, doc reference, and highlighted snippets) to the terminal. The formatter in Mix.Tasks.UsageRules.SearchDocs interpolated those publisher-controlled fields verbatim, neutralizing no terminal control characters; the only transform it applied adds escape sequences rather than removing them. A malicious package can embed ANSI terminal escape sequences (cursor movement, line erase, carriage returns, OSC 52 clipboard writes) in its indexed documentation, so when a developer runs a search that surfaces those docs the sequences reach the terminal unchanged — forging the displayed hexdocs URL or a suggested command, hiding text, or writing to the clipboard. No authentication or privileged position is required; only publishing a package. This issue affects usage_rules: from 0.1.18 before 1.2.8.	N/A	More Details
CVE-2026-12962	A Permissive Cross-domain Security Policy with Untrusted Domains in Armoury Crate allows a remote user to obtain a local user's NTLM hash by convincing the user to visit a crafted web page that sends a request containing a UNC path to the application's local service endpoint.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-16003	Exposed IOCTL with Insufficient Access Control in Armoury Crate driver allows a local user to add an arbitrary process identifier to the driver's whitelist via a crafted IOCTL request by bypassing the driver's verification.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-82514	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-16004	Exposed IOCTL with Insufficient Access Control in Armoury Crate driver allows a local user to read and write arbitrary PCI/PCIe configuration space via crafted IOCTL requests by bypassing the driver's verification. Refer to the ' Security Update for Armoury Crate App' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-16005	Release of Invalid Pointer or Reference in Armoury Crate driver allows a local user to free arbitrary memory via a crafted IOCTL request by bypassing the driver's verification, which can corrupt data structures and cause a system crash (BSOD).Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-16006	Exposure of Sensitive System Information to an Unauthorized Control Sphere in Armoury Crate driver allows a local user to obtain kernel virtual addresses via a crafted IOCTL request by bypassing the driver's verification, potentially providing further insight into the kernel memory layout.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-82584	Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in ash-project igniter allows a malicious package publisher to forge the mix igniter.install confirmation prompt. mix igniter.install prints a confirmation panel (an anti-typosquatting safeguard) listing a package's hex metadata before adding it. The panel builder in Igniter.Project.Deps wrote publisher-controlled fields (meta.description, owner usernames, requirement names, version) to the terminal with only newlines stripped. A malicious or typosquatted package can embed ANSI terminal escape sequences (cursor movement, line erase, carriage returns) in its metadata to overwrite the panel, forging trusted author names and download counts while concealing the real ones, so a developer relying on the panel to vet the package is deceived into approving a malicious dependency. This issue affects igniter: from 0.8.1 before 0.8.4.	N/A	More Details

CVE-2026-80746	In the Linux kernel, the following vulnerability has been resolved: clk: qcom: dispcc-eliza: Fix disp_cc_mdss_mdp_clk_src RCG stall on Eliza EVK Eliza EVK (eliza-cqs-evk.dts) does not have display enabled, however its Display Clock Controller is enabled and references parent clocks from DSI PHYs, which causes clock reparenting issues during probe (init) and warning on Eliza EVK: disp_cc_mdss_mdp_clk_src: rcg didn't update its configuration. WARNING: drivers/clk/qcom/clk-rcg2.c:136 at update_config+0xd4/0xe4, CPU#1: udevd/273 ... update_config (drivers/clk/qcom/clk-rcg2.c:136 (discriminator 2)) (P) clk_rcg2_shared_disable (drivers/clk/qcom/clk-rcg2.c:1471) clk_rcg2_shared_init (drivers/clk/qcom/clk-rcg2.c:1540) __clk_register (drivers/clk/clk.c:3959 drivers/clk/clk.c:4368) devm_clk_hw_register (drivers/clk/clk.c:4448 (discriminator 1) drivers/clk/clk.c:4672 (discriminator 1)) devm_clk_register_regmap (drivers/clk/qcom/clk-regmap.c:104) qcom_cc_really_probe (drivers/clk/qcom/common.c:418) qcom_cc_probe (drivers/clk/qcom/common.c:445) disp_cc_eliza_probe (dispcc-eliza.c:?) dispcc_eliza platform_probe (drivers/base/platform.c:1432)	N/A	More Details
CVE-2026-78325	Cross-site scripting in the Evernote and Google Keep note importers in Standard Notes for Android through 3.201.24 allows an attacker to execute arbitrary JavaScript in the application context when a victim imports a crafted .enex or Google Keep HTML file, leading to theft of encryption keys and note data, and arbitrary invocation of native device APIs.	N/A	More Details
CVE-2026-80764	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: fix LE list UAF on reset hci_cc_reset() clears the LE accept and resolving lists without taking hdev->lock. Other command-complete handlers serialize updates to these lists with that lock, and the debugfs readers hold it while walking them. This permits the reset completion and a debugfs read to interleave as follows: hci_rx_work debugfs reader ---------- ---------- lock hdev->lock fetch current entry list_del(entry) kfree(entry) read entry fields The reader then dereferences a freed list entry and may follow its stale next pointer. KASAN reported: BUG: KASAN: slab-use-after-free in white_list_show+0x15f/0x180 Read of size 1 at addr ffff8881015dab16 by task poc/95 Call Trace: white_list_show+0x15f/0x180 seq_read_iter+0x3ff/0x1190 seq_read+0x267/0x3d0 vfs_read+0x177/0xa20 ksys_read+0xf7/0x1c0 Allocated by task 91: hci_bdaddr_list_add+0x1a6/0x3a0 hci_cc_le_add_to_accept_list+0xab/0x140 hci_cmd_complete_evt+0x26c/0x9a0 hci_event_packet+0x454/0xb20 hci_rx_work+0x293/0x730 Freed by task 90: kfree+0x131/0x3c0 hci_bdaddr_list_clear+0xd8/0x160 hci_cc_reset+0x28a/0x370 hci_cmd_complete_evt+0x26c/0x9a0 hci_event_packet+0x454/0xb20 hci_rx_work+0x293/0x730 Take hdev->lock around both list clears. This matches the existing mutation and traversal locking convention.	N/A	More Details
CVE-2026-82729	Inefficient Algorithmic Complexity vulnerability in elixir-mint mint allows a remote HTTP server to exhaust CPU on the client host and cause a denial of service. parse_hex_prefix/2 in lib/mint/http1/parse.ex folds each hex digit of a chunked response's chunk-size field into an arbitrary-precision accumulator with acc * 16 + digit and imposes no limit on the digit count. Because the accumulator grows without bound, the multiplication is not constant time and one pass over N digits costs O(N squared). handle_data/2 prepends conn.buffer and re-parses from the start on every socket message, so a server that dribbles the digits out in small packets makes the client pay that cost repeatedly. A run of roughly 512,000 hex digits costs over ten seconds of CPU in a single pass, measured on stock defaults. The parser reaches this state after a valid status line and a complete, valid header section, so an intermediary inspecting only headers sees an ordinary 200 response. This issue affects mint: from 1.9.3 before 1.10.0.	N/A	More Details
CVE-2026-53600	async-tar is a tar archive reading/writing library for async Rust. Prior to version 0.6.1, async-tar mis-applies a buffered PAX size extension to an intermediary extension header (a GNU longname L, a GNU longlink K, or a PAX x/g header) instead of to the next file entry. POSIX requires a PAX extended-header record set to describe the next file entry, never an intervening extension header. Because poll_next_raw (src/archive.rs) threads the buffered PAX records into the size computation of whatever raw header it reads next — and that header can be an intermediary L — the stream cursor is advanced by an attacker-chosen amount when the L body is consumed. The parser then desyncs relative to a POSIX-correct tar parser (e.g. GNU tar), reading subsequent bytes at the wrong block boundary. This issue has been patched in version 0.6.1.	N/A	More Details
CVE-2026-82955	In the current development version of Eclipse aeriOS, which has not yet had an official release, the KrakenD instance included in the API Gateway component had the disable_jwk_security parameter hard-coded to true, with no option to override it through the Helm chart configuration. This setting disables TLS certificate verification when KrakenD retrieves the JSON Web Key Set (JWKS) used to validate bearer tokens, potentially allowing an attacker with the ability to intercept this communication to provide a malicious JWKS and compromise token validation. The issue has been addressed by making the parameter configurable through the boolean Helm value krakend.config.disableJwkSecurity and setting its default value to false, ensuring that TLS certificate verification is enabled by default.	N/A	More Details
CVE-2026-79991	Craft CMS GraphQL entry mutation resolvers (saveEntry, deleteEntry) read siteIddirectly from$argumentswithout passing throughArgumentManagerprepareArguments(), which is the function that enforces site-scope filtering via array_intersect against the GraphQL schema’s allowed sites. The query path (ElementResolverprepareElementQuery) correctly calls prepareArguments()`, so queries to unauthorized sites return empty. But mutations bypass this entirely — an attacker with a token scoped to Site A can create, modify, or delete entries in Site B by passing siteId in the mutations argument.	N/A	More Details
CVE-	Craft CMS GraphQL entry mutation resolvers (saveEntry, deleteEntry) read siteIddirectly from$argumentswithout passing throughArgumentManagerprepareArguments(), which is the function that		

2026-79990	enforces site-scope filtering via array_intersect against the GraphQL schema's allowed sites. The query path (ElementResolverprepareElementQuery) correctly calls prepareArguments()`, so queries to unauthorized sites return empty. But mutations bypass this entirely — an attacker with a token scoped to Site A can create, modify, or delete entries in Site B by passing siteId in the mutations argument.	N/A	More Details
CVE-2026-79989	The vulnerability allows any authenticated user to change their own password without providing the current password or having an active elevated session. It also allows the attacker to change other users' passwords if the attacker's account has Edit users permission (which doesn't allow changing others' passwords) and lacks Administrate users permission (which is required to change others' passwords).	N/A	More Details
CVE-2022-35497	In Trimble TM4WEB 21.4.0.4 due to security misconfiguration with session identifiers, it is possible to recover valid session cookies via reflected cross-site scripting affecting the external document viewer endpoint.	N/A	More Details
CVE-2026-75162	An information disclosure vulnerability in the opcua-configuration method of /cgi-bin/wwwugw.cgi in MBS-Solutions X-Serie Gateway firmware V6_00_05 allows any remote authenticated user, including users with the low-privileged Standard role, to retrieve the configured OPC-UA authentication credentials in cleartext via the JSON API response.	N/A	More Details
CVE-2026-75166	Insecure Permission vulnerability in MBS-Solutions X-Serie Gateway firmware V6_00_05 allows the low-privileged service user to execute /usr/bin/tcpdump as root without a password. By leveraging the tcpdump -z option, an authenticated attacker can achieve arbitrary command execution.	N/A	More Details
CVE-2026-75167	A broken access control vulnerability in the ugw-usr-edit method of /cgi-bin/wwwugw.cgi in MBS-Solutions X-Serie Gateway firmware V6_00_05 allows a remote authenticated user with the low-privileged Standard role to change the password of arbitrary accounts.	N/A	More Details
CVE-2026-75170	Cross-site scripting (XSS) vulnerability in the /loginController/doLogin endpoint of the HubCore platform (version 14.1.1) allows a remote unauthenticated attacker to inject arbitrary JavaScript into the application's response via the language POST parameter.	N/A	More Details
CVE-2026-75171	An issue in HubCore v.14.1.1 allows a remote attacker to escalate privileges via the HUBCOREID session cookie handling component.	N/A	More Details
CVE-2026-75429	PowerJob versions 4.x through 5.1.2 contain an unauthenticated remote code execution vulnerability in the /friend/process endpoint of the Server-Worker transport layer	N/A	More Details
CVE-2026-79419	A reflected cross-site scripting (XSS) vulnerability exists in EMX Tecnologia Gestao X Business Suite 8.4 and earlier. The vulnerability is caused by insufficient validation and sanitization of the mensagem parameter in the /Configuracao/Imagens.aspx endpoint, allowing an authenticated attacker to inject arbitrary JavaScript code that is reflected and executed in the context of a victim's browser.	N/A	More Details
CVE-2026-80758	In the Linux kernel, the following vulnerability has been resolved: futex: Avoid private hash use-after-free on final put futex_private_hash_put() drops the reference to fph before evaluating fph->mm for wake_up_var(). futex_ref_put() enables preemption again before returning. If that put drops the final reference and the task is preempted, another task can pivot to the replacement hash and free the old hash after an RCU grace period. The first task then reads fph->mm from the freed allocation when it resumes. KASAN reports a slab-use-after-free in futex_private_hash_put(), with the read at offset 24 in a freed kmalloc-512 allocation. The allocation and free stacks point to futex_hash_allocate() and the RCU free path, respectively. Load the mm pointer while the fph reference is still held and pass the saved value to wake_up_var(). wake_up_var() uses the pointer as a waitqueue key and does not dereference the mm through it.	N/A	More Details
CVE-2026-80759	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_aml: validate firmware segment lengths aml_download_firmware() reads two lengths from the firmware header and uses them to build pointers before checking that the header and segment data are present. A truncated or inconsistent firmware image can make the driver read past firmware->data while constructing TCI commands. Reject images shorter than the header and ensure that the ICCM and DCCM ranges fit within the loaded firmware before downloading either segment.	N/A	More Details
CVE-2026-80760	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: reject HCI_CMD_SYNC params_len above 255 mgmt_hci_cmd_sync() checks that the message length agrees with params_len but puts no upper bound on it. params_len is __le16 while the parameter length in the HCI command header is a u8: struct hci_command_hdr { __le16 opcode; __u8 plen; } __packed; hci_cmd_sync_alloc() assigns one to the other: hdr->plen = plen; if (plen) skb_put_data(skb, param, plen); so a params_len of 256 leaves plen at 0 while all 256 bytes are still appended. The frame handed to the driver then declares no parameters and carries 256 of them. On a length framed transport such as H:4 the controller takes the trailing bytes as the start of the next packet. The mgmt socket MTU is HCI_MAX_FRAME_SIZE, so params_len can reach about 1KB this way. Commit 03f1700b9b4d ("Bluetooth: MGMT: reject malformed HCI_CMD_SYNC commands") only made params_len agree with the message length, a value that fits the message but not the header field is still accepted. Reject params_len that does not fit the header field.	N/A	More Details

CVE-2026-80761	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: zero the sockaddr before returning it in getname iso_sock_getname() fills a struct sockaddr_iso in place and returns its size without clearing it first, so bytes it does not write are copied to user space from the kernel stack. The getsockname(2) and getpeername(2) paths both run through do_getsockname(), which hands getname() an uninitialized sockaddr_storage on the stack and copies back up to the number of bytes getname() returns, so the driver has to initialize every byte it accounts for. Two ranges are left uninitialized: - struct sockaddr_iso is 10 bytes but only 9 are written (family, iso_bdaddr, iso_bdaddr_type), leaking the trailing pad byte on every call. - for a broadcast peer (BIS_LINK or PA_LINK) the returned length grows by sizeof(struct sockaddr_iso_bc), but only bc_sid, bc_num_bis and bc_bis are filled; bc_bdaddr and bc_bdaddr_type, the first 7 bytes of that structure, are never written. An unprivileged process can open a BTPROTO_ISO socket and reach the pad leak with getsockname(); the broadcast leak needs an established BIS/PA connection. l2cap and rfcomm already memset their sockaddr in getname for the same reason; do the same here.	N/A	More Details
CVE-2026-80762	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: Fix accept list UAF during suspend hci_update_event_filter_sync() walks hdev->accept_list while sending a synchronous HCI command for each remote-wakeup device. The suspend path holds hdev->req_lock, but accept-list updates are serialized by hdev->lock. Consequently, remove_device() can free the current list entry during the controller wait. The following interleaving causes the use-after-free: hci_update_event_filter_sync() remove_device() fetch accept-list entry hci_set_event_filter_sync() wait for controller response hci_dev_lock() list_del() kfree() hci_dev_unlock() read the freed list.next KASAN reported: BUG: KASAN: slab-use-after-free in hci_suspend_sync+0x835/0x910 Read of size 8 at addr ffff88810bec8440 by task kworker/0:1/10 Workqueue: events vhci_suspend_work Call Trace: hci_suspend_sync+0x835/0x910 hci_suspend_dev+0x182/0x450 process_one_work+0x661/0x1090 worker_thread+0x45b/0xd10 Allocated by task 86: hci_bdaddr_list_add_with_flags+0x1a8/0x400 add_device+0x381/0x820 hci_sock_sendmsg+0x1033/0x1ea0 Freed by task 91: kfree+0x131/0x3c0 remove_device+0x429/0xb70 hci_sock_sendmsg+0x1033/0x1ea0 Snapshot the remote-wakeup addresses under hdev->lock. Release the lock before sending HCI commands. Clear the controller event filter before building the snapshot, and skip allocation and the second list traversal when there are no matching entries. This preserves the original filter and scan-state updates without retaining an accept-list node across a controller wait.	N/A	More Details
CVE-2026-82728	Allocation of Resources Without Limits or Throttling vulnerability in elixir-mint mint allows a remote HTTP server to exhaust memory on the client host and cause a denial of service. Two HTTP/1 response-parser states accumulate server data without any cap. In lib/mint/http1.ex, decode_status_line/4 stores the unconsumed data in conn.buffer when the status line is incomplete, and decode_body/5 does the same for an unterminated chunk-extension line. Both wait for a CRLF the server never has to send, and conn.buffer is prepended to every subsequent socket message. The :max_header_list_size budget is wired only into decode_headers/5 and decode_trailer_headers/4, so neither of these states is covered by it. A malicious server, or one reached through an attacker-controlled redirect or a fetched URL, streams bytes indefinitely until the BEAM node is killed by the operating system out-of-memory handler. The chunk-extension variant is reached after a valid status line and a complete, valid header section, so an intermediary inspecting only headers sees an ordinary 200 response. This issue affects mint: from 0.1.0 before 1.10.0.	N/A	More Details
CVE-2026-85597	Traefik before v2.11.55 and v3.0.0 through v3.7.10 contain a TLS option conflict resolution vulnerability that allows unauthenticated attackers to bypass client-certificate authentication by creating conflicting TLS options on multi-host routers. Attackers can reach protected backends by exploiting shared TLS resolution across multiple hostnames in a single router rule, causing the strict mTLS requirement to fall back to default options for all hosts.	N/A	More Details
CVE-2026-85596	Traefik versions >= v3.7.0 and <= v3.7.10 contain an authentication bypass in the Kubernetes Ingress NGINX provider. The TLS option generated for an Ingress carrying the nginx.ingress.kubernetes.io/auth-tls-secret annotation was named after the Ingress namespace and name. As a result, two Ingress objects sharing the same host, the same client CA secret, and the same client-authentication mode produced two distinct TLS option names for that host. Traefik treats this as a TLS options conflict and falls back to the entry point's default TLS configuration, which does not request a client certificate, so a route configured with nginx.ingress.kubernetes.io/auth-tls-verify-client: "on" becomes reachable without a client certificate. Only the v3.7 line is affected; the issue is fixed in v3.7.11.	N/A	More Details
CVE-2026-85547	A cross-site request forgery (CSRF) vulnerability exists in MISP due to form-security and CSRF protections being disabled based on whether an incoming request was identified as a REST request. MISP's REST detection can be influenced by request properties such as the URL suffix or the HTTP Accept header. Because Accept: application/json can be supplied by a cross-origin page without requiring a CORS preflight, an attacker could cause a request originating from another website to be treated as REST traffic. MISP would consequently disable its normal form-security and CSRF validation even though the request was authenticated using the victim's existing browser session. An unauthenticated remote attacker could exploit this behavior by convincing an authenticated MISP user to visit or interact with a malicious web page. The attacker's page could then issue crafted requests to susceptible state-changing MISP endpoints using the victim's privileges. Depending on the permissions of the victim and the targeted endpoint, this could allow unauthorized modification, creation, publication, or removal of data and other state changes. The vulnerability originates from granting the form-security exemption based on _isRest() rather than on the authentication mechanism used by the request. The patch changes this behavior so that CSRF and form-	N/A	More Details

	security exemptions are granted only when the request actually carries a MISP API key. Session-authenticated REST-style requests remain subject to CSRF protection. The fix also introduces support for transmitting CSRF tokens through the X-CSRF-Token header for legitimate same-origin AJAX requests. Such a header cannot normally be attached by a cross-origin page without triggering a CORS preflight, preventing it from being used to reproduce the original attack.		
CVE-2026-84376	Astro is a web framework for content-driven websites. Prior to 7.2.4, Astro stripped a configured non-root base path from request pathnames using a string-prefix check without verifying a path-segment boundary. With base "/app", a request to "/appX/admin" resolved internally to the protected "/admin" route while middleware observed "/appX/admin" in context.url.pathname. In applications that authorize base-prefixed routes by inspecting context.url.pathname, an unauthenticated remote attacker could bypass pathname-based middleware authorization and reach protected routes. This issue is fixed in version 7.2.4.	N/A	More Details
CVE-2026-81302	PALLET CONTROL products contain an incorrect default permission vulnerability, which may allow a local attacker to execute arbitrary code with SYSTEM privileges on the affected product.	N/A	More Details
CVE-2026-79756	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. Prior to version 1.17.4, the fix for unauthenticated OS command injection in the nuclio dashboard on the local/Docker platform is incomplete. The fix added validateFunctionName for function names and common.Quote() for the named-resource shell command path, but the list-all resource path (triggered when no specific resource name is provided) still interpolates the resourceNamespace parameter unquoted into a /bin/sh -c command string. An unauthenticated attacker can inject shell metacharacters via the X-Nuclio-Function-Namespace, X-Nuclio-Project-Namespace, or X-Nuclio-Function-Event-Namespace HTTP headers to achieve arbitrary command execution inside the dashboard container. This issue has been patched in version 1.17.4.	N/A	More Details
CVE-2026-85533	An authorization flaw in MISP allowed an authenticated user to submit a sharing_group_id without verifying that the user was authorized to use the referenced Sharing Group. In several attribute and Galaxy Cluster creation and editing workflows, validation of the submitted Sharing Group was performed only when the request explicitly set the distribution field to 4 ("Sharing Group"). An attacker could therefore craft a request containing a sharing_group_id while omitting the distribution parameter, or otherwise avoiding the distribution == 4 condition, causing the Sharing Group authorization check to be skipped. This could allow a user with permission to create or modify the affected MISP objects to associate data with a Sharing Group that they are not authorized to use. Depending on the affected object's existing distribution settings and subsequent processing, this could bypass intended information-sharing boundaries and result in unauthorized placement or distribution of data to members of another Sharing Group. The issue affected attribute attachment and editing operations as well as Galaxy Cluster creation and editing. The fix ensures that authorization is performed whenever a non-empty sharing_group_id is submitted, independently of the distribution parameter. It also centralizes the authorization decision in SharingGroup::canUse() and explicitly rejects empty Sharing Group identifiers rather than allowing them to be interpreted as an unrestricted query.	N/A	More Details
CVE-2026-85538	An incorrect authorization vulnerability in MISP allowed authenticated users to delete attributes from events despite lacking the required perm_modify or perm_modify_org permissions. The affected attribute deletion paths relied on organization membership checks performed by MispAttribute::deleteAttribute() but did not consistently enforce MISP's event modification authorization rules. Consequently, a user belonging to the organization associated with an event could potentially delete individual attributes or perform bulk attribute deletion even when their assigned role was not authorized to modify the event. This created an inconsistency between attribute editing and deletion: editing an attribute correctly used MISP's ACL::canModifyEvent() authorization logic, whereas the affected deletion operations could bypass these permission checks. An authenticated attacker with access to an affected MISP instance and membership in the organization owning an event could exploit this flaw to remove attributes from that event, potentially causing unauthorized modification or loss of threat intelligence data. The patch introduces a common authorization check for all affected deletion paths. Before deletion, MISP now resolves the associated events and verifies that the current user is authorized to modify each event using the same authorization mechanism used by normal event and attribute modification operations.	N/A	More Details
CVE-2026-13148	Missing release of memory after effective lifetime vulnerability in Softing smartLink allows resource leak exposure. This issue affects smartLink HW-PN: from 1.04 before 1.10.	N/A	More Details
CVE-2026-79754	Nuclio is a "Serverless" framework for Real-Time Events and Data Processing. From version 1.6.19 to before version 1.17.2, Nuclio's Dashboard build pipeline does not sanitize the spec.build.tempDir field before using it to construct a shell command. When the Kaniko container builder is enabled, a user with function-create permission can inject shell metacharacters into this field and achieve arbitrary command execution inside the Dashboard container, which runs with a Kubernetes service account holding wildcard access to Secrets, Pods, Jobs, and Deployments in its namespace. This issue has been patched in version 1.17.2.	N/A	More Details
	MISP contains a cross-site request forgery (CSRF) vulnerability in the sharing group quick-edit functionality. The addOrg, removeOrg, addServer, and removeServer actions share the __initialiseSGQuickEdit() helper, where the HTTP method validation intended to restrict these operations to POST requests was commented out. As a result, these state-changing actions could be invoked using GET requests. An attacker could craft a		

CVE-2026-85546	URL targeting one of the affected actions and cause an authenticated MISP user with sufficient privileges to request it, for example through a malicious link or embedded web resource. Successful exploitation could modify the membership of a MISP sharing group without the victim intentionally performing the operation. Depending on the action performed, an attacker could add or remove organisations or servers from a sharing group, potentially granting unintended access to information distributed through that sharing group or disrupting legitimate information sharing. The patch restores HTTP method enforcement centrally in __initialiseSGQuickEdit() by calling allowMethod(['post']), ensuring that all four affected quick-edit operations require POST requests and are therefore subject to the application's normal protections for state-changing requests.	N/A	More Details
CVE-2026-4644	A Missing Authorization vulnerability in HTTP Connector in Google Cloud Integration Connectors versions prior to 2025-12-11 on Google Cloud Platform allows an authenticated user to escalate privileges and take over a Google Cloud Project using unauthorized service account attachment. This vulnerability was patched on 11 December 2025, and no customer action is needed.	N/A	More Details
CVE-2026-85595	Traefik versions before v2.11.55 and versions v3.0.0 through v3.7.10 contain an authentication bypass vulnerability in the digestAuth middleware where unknown usernames receive an empty secret instead of rejection. Attackers can compute a valid digest response using the empty secret and arbitrary credentials to bypass authentication on any digestAuth-protected route without a valid username or password.	N/A	More Details
CVE-2026-79707	A Path Traversal vulnerability in the builder endpoint in Google Cloud Agent Development Kit (ADK) versions 1.9.0 through 1.21.0 on Python allows an unauthenticated remote attacker to read arbitrary files using a crafted file_path query parameter.	N/A	More Details
CVE-2026-85586	phpMyFAQ versions before 4.1.8 fail to validate CAPTCHA when the store parameter is set to 'now' in question submission requests. Unauthenticated attackers can bypass CAPTCHA protection and submit unlimited questions directly, causing database pollution and triggering outgoing mail notifications.	N/A	More Details
CVE-2026-85587	phpMyFAQ before 4.1.8 enforces incorrect permission checks on admin content pages, allowing lesser-privileged editors to read draft and inactive content. Attackers with only add permissions can access news edit and FAQ translate endpoints to view unpublished content invisible to the public.	N/A	More Details
CVE-2026-85588	phpMyFAQ versions before 4.1.8 include live TOTP shared secrets in plaintext within user data export ZIP files. Attackers obtaining exported archives can extract the TOTP seed and generate valid one-time codes to bypass two-factor authentication.	N/A	More Details
CVE-2026-85589	phpMyFAQ before 4.2.0-alpha.2 contains a missing authorization vulnerability in the admin dashboard API endpoints searches and content-health that enforce only authentication without permission checks. Any authenticated user can access these endpoints to read site-wide search statistics and content-health counters regardless of their privilege level.	N/A	More Details
CVE-2026-85590	phpMyFAQ before 4.1.8 contains an authentication bypass vulnerability in its two-factor authentication (TOTP) disable functionality. The removeTwofactorConfig() handler (reachable via POST /api/user/remove-twofactor) verifies only that the user is logged in and that a valid CSRF token is supplied, then disables TOTP without requiring password re-entry or a current TOTP code. The same downgrade is also reachable inline via PUT /api/user/data/update, which accepts a plain twofactor_enabled form field under the same session+CSRF-only guard. An attacker who has hijacked a user's session can silently strip two-factor protection from any account, including administrator accounts, after which password-only authentication succeeds.	N/A	More Details
CVE-2026-85591	phpMyFAQ versions before 4.1.8 contain an authentication bypass vulnerability in the user control panel API endpoint that allows authenticated attackers to change account passwords without verifying the current password. Attackers with session access can submit a PUT request to the user data update endpoint with only a CSRF token to silently change any user's password, including administrators, causing irreversible account takeover and victim lockout.	N/A	More Details
CVE-2026-85594	Traefik versions from v3.7.1 fail to enforce crossProviderNamespaces restrictions on the traefik.ingress.kubernetes.io/service.middlewares Service annotation in the Kubernetes Ingress provider. A namespace-limited tenant excluded from the allowlist can attach an operator-owned middleware to its Service, and if that middleware injects backend credentials, recover them at a controlled backend.	N/A	More Details
CVE-2026-80763	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_event: validate LE Set CIG Parameters response The Command Complete dispatch validates only the fixed part of the LE Set CIG Parameters response. After that part is pulled from the skb, hci_cc_le_set_cig_params() trusts num_handles and reads each entry in the trailing handle array. Matching num_handles against the command's num_cis does not guarantee that the response contains the advertised handles. A truncated response from a malfunctioning controller can therefore make the handler read beyond the skb data. Validate that the remaining skb data contains all advertised handles. Include this in the existing response validation so malformed responses also follow the established CIG failure handling.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: HID: hyperv: validate initial device info bounds The Hyper-V synthetic HID host supplies SYNTH_HID_INITIAL_DEVICE_INFO messages that contain a HID descriptor followed by the report descriptor bytes. mousevsc_on_receive_device_info() trusts bLength		

CVE-2026-80765	and wDescriptorLength without checking that the received packet contains both byte ranges. A malformed host or backend message can therefore make the guest read past the received VMBus packet while copying the report descriptor. Pass the received initial-device-info size into the parser and reject descriptor lengths that exceed the packet. Impact: A malicious Hyper-V host or backend can crash a guest by sending a short initial device-info message with an oversized HID report descriptor length.	N/A	More Details
CVE-2026-86351	Affected versions of MISP validate the user-configurable homepage by checking only whether the supplied path begins with /. That check is insufficient because protocol-relative URLs such as //attacker.example also begin with / but resolve to an external origin in browsers. The vulnerable homepage value can be stored as a user setting and later used by the post-login routing logic. The commit explicitly identifies //attacker.example as a payload that passed validation and was emitted to the Location header after login. The fix introduces a shared InternalRedirectValidator that rejects URLs containing a host, scheme, userinfo, unsafe leading // or /\, malformed URLs, and control characters. It also revalidates homepage settings on read so legacy or internally written unsafe values cannot bypass the new storage-time validation. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-80766	In the Linux kernel, the following vulnerability has been resolved: HID: uclogic: fix use-after-free of inrange_timer on remove uclogic_remove() cancels the pen in-range timer and then stops the device: timer_delete_sync(&drvdata->inrange_timer); hid_hw_stop(hdev); timer_delete_sync() only guarantees the timer is idle at that instant. uclogic_raw_event_pen() keeps delivering pen reports until hid_hw_stop() stops the transport several lines later, and every report with pen->inrange == UCLOGIC_PARAMS_PEN_INRANGE_NONE re-arms the timer: mod_timer(&drvdata->inrange_timer, jiffies + msecs_to_jiffies(100)); A report landing between the timer_delete_sync() call and the transport teardown in hid_hw_stop() re-arms inrange_timer after it was cancelled. uclogic_remove() then returns and the devm drvdata is freed, while hid_hw_stop() has already freed the input device drvdata->pen_input points at, so when the timer fires ~100 ms later uclogic_inrange_timeout() dereferences freed memory -- a use-after-free in timer-softirq context. Swapping the two calls is not a fix: stopping the device first frees drvdata->pen_input via hidinput_disconnect() while the timer may still be pending, so a timer already armed before removal fires on the freed input device in the window before timer_delete_sync() runs. Use timer_shutdown_sync() before hid_hw_stop() instead. It cancels the timer, waits for a running callback while pen_input is still valid, and prevents any further re-arming -- a later mod_timer() from an in-flight report is silently ignored -- so the timer is provably dead before hid_hw_stop() frees the inputs. This is the ordering the timer core documents for this "timer re-armed from another path" teardown case.	N/A	More Details
CVE-2026-80789	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: bound SGL data length before allocating command buffers nvmet_tcp_map_data() reads the host-controlled 32-bit sgl->length and, for the in-capsule offset descriptor (type 0x01), checks it against port->inline_data_size before use. Any other SGL descriptor type -- including the non-inline transport SGL data-block descriptor (type (NVME_TRANSPORT_SGL_DATA_DESC << 4) | NVME_SGL_FMT_TRANSPORT_A, the type a real host uses for out-of-capsule writes) skips that check entirely and falls straight through to: cmd->req.sg = sgl_alloc(len, GFP_KERNEL, &cmd->req.sg_cnt); with len taken directly from the wire, unbounded up to 4 GiB. nvmet_req_init() only parses the command and never inspects sgl->length, and nvmet_check_transfer_len() -- the only other place transfer_len is validated -- runs later, from req->execute(), after the allocation has already happened. For a write command the target responds with an R2T and parks the command waiting for the host to send the data; if the host (or an unauthenticated peer that simply never follows up) never does, the sgl_alloc() buffer stays resident for the life of the command. NVMe/TCP has no mandatory authentication in the default configuration, so any peer able to reach the target portal and complete a Fabrics connect can drive this with a single crafted command, repeatable across queues and connections for amplification. This is unbounded kernel memory allocation triggered by a remote, effectively unauthenticated peer. Validate len against the same NVMET_TCP_MAXH2CDATA ceiling this file already uses to bound per-PDU H2C data, for every SGL descriptor type, before doing any allocation. This closes the gap for the non-inline descriptor while leaving the existing, tighter inline_data_size check in place for the in-capsule case. Runtime-verified on a v6.19 KASAN stand: with this bound in place, a crafted write command carrying an oversized non-inline SGL length is rejected before sgl_alloc() runs, where the same request previously drove an unbounded ~256 MiB kernel allocation (up to 4 GiB) that stayed resident pending an R2T the host never satisfies.	N/A	More Details
CVE-2026-80790	In the Linux kernel, the following vulnerability has been resolved: nvmet-fc: fix invalid free in LS IOD error path nvmet_fc_alloc_ls_iodlist() advances iod while initializing the LS IOD array. If an rqstbuf allocation or response buffer DMA mapping fails, the unwind loop decrements iod past the start of the array. The final kfree(iod) therefore frees an address before the allocated object. This can be reproduced with nvme-fcloop and failslab by setting fail-nth to 6 before creating a target port. KASAN reports: BUG: KASAN: invalid-free in nvmet_fc_register_targetport Free of addr ffff88816cf8ff48 by task nvmet_fail_nth/9552 Free the original allocation base stored in tgtport->iod instead. With this fix applied, the same sysfs write with fail-nth=6 returns -ENOMEM without any KASAN report.	N/A	More Details
CVE-2026-80791	In the Linux kernel, the following vulnerability has been resolved: nvmet-auth: zero the AUTH_RECEIVE response buffer nvmet_execute_auth_receive() allocates the response buffer with kmalloc() sized by the host-supplied AUTH_RECEIVE allocation length, but the DH-HMAC-CHAP builders write only a fixed-size message into it. The full allocation length is then copied to the wire by nvmet_copy_to_sgl(), so a remote initiator receives the bytes past the built message -- up to nearly a page of uninitialized slab -- during the pre-authentication handshake. Allocate the buffer with kzalloc() so the unwritten tail is zeroed before it is sent;	N/A	More Details

	conforming responses are unaffected.		
CVE-2026-80792	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix use-after-free in ip6_finish_output2() ip6_finish_output2() caches a pointer to the IPv6 destination address (daddr) before invoking lwtunnel_xmit(). The LWT-BPF transmit path or other encapsulation operations within lwtunnel_xmit() can reallocate the skb head, freeing the memory that daddr points to. When lwtunnel_xmit() returns LWTUNNEL_XMIT_CONTINUE, the function continues to use the stale daddr pointer to compute the nexthop and to look up or create the neighbour entry. This results in a use-after-free read, which can leak sensitive kernel data, pollute the neighbour table with arbitrary values, misdirect traffic, or crash the system. Fix this by re-fetching the IPv6 header and the destination address pointer after lwtunnel_xmit() returns LWTUNNEL_XMIT_CONTINUE, ensuring that the subsequent nexthop computation and neighbour lookup operate on valid memory.	N/A	More Details
CVE-2026-80793	In the Linux kernel, the following vulnerability has been resolved: ipv4: reject undersized MTUs in ip_do_fragment() ip_do_fragment() subtracts the IPv4 header length from the effective MTU and passes the resulting payload MTU to ip_frag_next(). If the effective MTU is smaller than hlen + 8, ip_frag_next() rounds the fragment payload length down to zero. The fragmentation state then never makes forward progress: state->left, state->ptr and state->offset stay unchanged while ip_do_fragment() keeps allocating and transmitting header-only fragments until the softlockup detector fires. This is reproducible with a route installed using "mtu lock 20", but it is also reproducible without route MTU lock, for example by forwarding a packet to a device whose MTU is 20. Fix it in ip_do_fragment() by rejecting mtu < hlen + 8 with -EMSGSIZE, matching the existing IPv6 fragmentation check.	N/A	More Details
CVE-2026-80794	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: fix uninit-value in the RF discover/activated NTF handlers nci_rf_discover_ntf_packet() and nci_rf_intf_activated_ntf_packet() each parse a notification into an on-stack struct (nci_rf_discover_ntf / nci_rf_intf_activated_ntf) that is not initialised. The RF technology-specific parameters are only extracted when rf_tech_specific_params_len is non-zero, so a notification that reports a zero length leaves the rf_tech_specific_params union uninitialised - and both handlers then pass it to nci_add_new_protocol(), which reads it: - discover: nci_add_new_target() -> nci_add_new_protocol(); - activated: nci_target_auto_activated() -> nci_add_new_protocol(). nci_add_new_protocol() uses nfca_poll->nfcid1_len as both a branch condition and a memcpy() length and copies nfcid1/sens_res/sel_res into ndev->targets, which is later exposed to user space via NFC_CMD_GET_TARGET. BUG: KMSAN: uninit-value in nci_add_new_protocol+0x624/0x6c0 nci_add_new_protocol+0x624/0x6c0 nci_ntf_packet+0x25b2/0x3c30 nci_rx_work+0x318/0x5d0 process_scheduled_works+0x84b/0x17a0 worker_thread+0xc10/0x11b0 kthread+0x376/0x500 Local variable ntf.i created at: nci_ntf_packet+0xbc2/0x3c30 Zero-initialise both on-stack notifications so the union reads back as zero when no technology-specific parameters are present.	N/A	More Details
CVE-2026-80795	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: fix out-of-bounds write in nci_target_auto_activated() nci_target_auto_activated() appends a target to the fixed-size array ndev->targets[NCI_MAX_DISCOVERED_TARGETS] and increments ndev->n_targets without first checking the array is full; unlike its sibling nci_add_new_target(), which bails out when n_targets already equals NCI_MAX_DISCOVERED_TARGETS. ndev->n_targets is only cleared by nci_clear_target_list(), so an NFCC that repeatedly re-runs discovery (RF_DISCOVER_RSP, which re-enters NCI_DISCOVERY without clearing the target list) and reports an auto-activated target (RF_INTF_ACTIVATED_NTF) drives n_targets past the limit. The append then writes a struct nfc_target past the end of the array (a slab out-of-bounds write), and nfc_targets_found() goes on to walk the array with the inflated count: BUG: KASAN: slab-out-of-bounds in nci_add_new_protocol+0x94/0x2ac [nci] Write of size 2 at addr ffff0000c7299a18 by task kworker/u8:0/12 Workqueue: nfc0_nci_rx_wq nci_rx_work [nci] Call trace: nci_add_new_protocol+0x94/0x2ac [nci] nci_ntf_packet+0xddc/0x11a0 [nci] nci_rx_work+0x15c/0x1e0 [nci] process_one_work+0x2dc/0x500 worker_thread+0x240/0x460 kthread+0x1c0/0x1d0 ret_from_fork+0x10/0x20 The buggy address belongs to the cache kmalloc-2k of size 2048 The buggy address is located 1024 bytes to the right of allocated 1560-byte region [ffff0000c7299000, ffff0000c7299618) Guard nci_target_auto_activated() with the same check used by nci_add_new_target().	N/A	More Details
CVE-2026-80796	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: add data_len bound checks to activation parameter extractors nci_extract_activation_params_iso_dep() and nci_extract_activation_params_nfc_dep() read an inner length byte from the NCI RF_INTF_ACTIVATED_NTF payload and use it to memcpy() into fixed kernel buffers, but neither function receives the caller-validated activation_params_len. A crafted NCI notification with activation_params_len=1 and an inner length byte of up to 20 (NFC-A) or 50 (NFC-B) causes memcpy() to read that many bytes past the one valid byte in the activation params region -- a slab out-of-bounds read of kernel memory adjacent to the NCI skb. The sibling nci_extract_rf_params_*() family was given equivalent protection by commit 571dcbeb8e63 ("net: nfc: nci: Fix parameter validation for packet data"), but the two activation parameter extractors were not updated at that time. Add a data_len parameter to both functions, guard against an empty region before consuming the inner length byte, decrement the remaining count after consuming it, and clamp the copy length to what is actually available. Update both call sites to pass ntf.activation_params_len, which is already validated against the skb at ntf.c:801.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nfc: pn533: purge fragmented skbs during cleanup pn53x_common_clean() purges resp_q before freeing the common PN533 state, but it leaves		

CVE-2026-80797	fragment_skb untouched. The fragmentation helpers queue transmit fragments there while sending large initiator or target-mode frames, and those skbs remain owned by the driver until they are sent or discarded. If the device is removed while fragments are still queued, the common cleanup path frees the PN533 state without releasing the queued fragment skbs, leaking them. Purge fragment_skb during cleanup alongside resp_q.	N/A	More Details
CVE-2026-80798	In the Linux kernel, the following vulnerability has been resolved: nfc: llcp: reject PDUs shorter than the LLCP header Every LLCP PDU begins with a two-byte header (DSAP/SSAP + PTYPE), but the receive path never checked that a frame is at least LLCP_HEADER_SIZE bytes before parsing it. nfc_llcp_rx_skb() reads the header via nfc_llcp_ptype()/nfc_llcp_dsap()/ nfc_llcp_ssap(), which dereference pdu->data[0] and pdu->data[1], and a CONNECT or CC PDU then computes tlv_array_len = skb->len - LLCP_HEADER_SIZE; as a size_t and hands it to the TLV walk. When the frame is shorter than the header the subtraction wraps to a huge value and the walk runs far past the buffer, an out-of-bounds read. A nearby NFC device can reach this without authentication; LLCP link activation happens automatically after NFC-DEP. Guard the common receive choke point __nfc_llcp_recv(), shared by both the target (nfc_llcp_data_received()) and initiator (nfc_llcp_recv()) paths, so a short skb is dropped before the rx_work worker parses it. Use pskb_may_pull() rather than a skb->len test so the two header bytes are guaranteed to sit in the skb linear area even for a non-linear skb, matching how the sibling NCI and HCI receive paths validate their headers. Reproduced with a KFENCE out-of-bounds read via /dev/virtual_nci on linux-next. Found by 0sec automated security-research tooling (https://0sec.ai).	N/A	More Details
CVE-2026-80799	In the Linux kernel, the following vulnerability has been resolved: nfc: llcp: fix OOB read and u8 offset wrap in TLV parsers nfc_llcp_parse_gb_tlv() and nfc_llcp_parse_connection_tlv() contain three related bugs in their TLV parsing loops: 1. 'offset' is declared u8 but tlv_array_len is u16. When TLV data advances offset past 255 it silently wraps to zero, causing infinite loops or double-processing of buffer data. 2. Before reading tlv[0] (type) and tlv[1] (length) there is no check that offset+2 <= tlv_array_len. A truncated TLV causes an OOB read of one byte past the buffer end. 3. After reading the length field, the value bytes are accessed without checking offset+2+length <= tlv_array_len. A crafted length=0xFF on a short buffer causes up to 255 bytes of OOB read past the buffer end. Both functions are reachable without authentication via nfc_llcp_set_remote_gb() which feeds remote LLCP general bytes directly into nfc_llcp_parse_gb_tlv() with no additional validation. Fix all three issues by widening offset from u8 to u16 and adding bounds checks for both the TLV header and value field before each access.	N/A	More Details
CVE-2026-80800	In the Linux kernel, the following vulnerability has been resolved: nfc: llcp: bound the connect_sn TLV walk to the skb Commit 27256cdb290e ("nfc: llcp: bound SNL TLV parsing to the skb and add length checks") fixed the unbounded TLV walk in nfc_llcp_recv_snl(), and commit d8bd2dedbde5 ("nfc: llcp: fix OOB read and u8 offset wrap in TLV parsers") subsequently bounded nfc_llcp_parse_gb_tlv() and nfc_llcp_parse_connection_tlv(). One sibling parser sharing the same pattern remains unbounded: nfc_llcp_connect_sn(). nfc_llcp_connect_sn() walks a TLV list, reading a two-byte header (type, length) followed by length bytes of value, without checking that the two header bytes or the declared length stay within the buffer. It returns a pointer to a service name of up to 255 bytes that may point past the end of the skb; it is subsequently consumed by memcmp() in nfc_llcp_sock_from_sn(). In addition tlv_array_len was computed as "skb->len - LLCP_HEADER_SIZE" in size_t, so a CONNECT/CC frame shorter than the LLCP header underflows to a huge length and the walk runs far past the buffer. nfc_llcp_connect_sn() is reachable from nfc_llcp_recv_connect() and nfc_llcp_recv_cc(), i.e. from received CONNECT and CC PDUs. A nearby NFC device can reach this without authentication; LLCP link activation happens automatically after NFC-DEP, and the nfc_llcp_rx_skb() dispatcher applies no minimum-length guard. Walk the TLV list by pointer, bounded by skb_tail_pointer(skb), and validate each declared length before use, matching the approach already used for nfc_llcp_recv_snl(). Starting the walk at &skb->data[LLCP_HEADER_SIZE] against the tail pointer also removes the size_t underflow for short frames. Found by 0sec automated security-research tooling (https://0sec.ai).	N/A	More Details
CVE-2026-80801	In the Linux kernel, the following vulnerability has been resolved: nfc: microread: validate target discovery payload lengths microread_target_discovered() parses target discovery payloads from skb->data according to the HCI gate. The fixed field offsets and UID copies were checked only against the destination nfc_target buffers, not against the actual skb length. Validate that each gate-specific payload contains the fixed fields and UID bytes before reading or copying them.	N/A	More Details
CVE-2026-80802	In the Linux kernel, the following vulnerability has been resolved: nfc: fdp: bound the device-reported read length and fix an skb leak fdp_nci_i2c_read() takes the next packet length from two device-supplied bytes and never validates it. The value is a u16 used as the i2c_master_recv() count into a 261-byte on-stack buffer: a malicious, counterfeit or malfunctioning controller (or an i2c bus interposer) can drive it far past the buffer for a stack out-of-bounds write that clobbers the canary and return address, or below the minimum frame size (directly, or by truncating the computed sum) so the header/LRC strip and the next length read run past a short receive. Reject a length outside [FDP_NCI_I2C_MIN_PAYLOAD, FDP_NCI_I2C_MAX_PAYLOAD], as a corrupted packet already is, and force resynchronization. The same loop allocates one data skb per iteration and assumes a length packet followed by a data packet; a device that sends two data packets in one call leaks the first skb when the second allocation overwrites it. Free a previously allocated skb before allocating the next.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nfc: digital: clamp SENSF_RES length to the destination buffer digital_in_recv_sensf_res() memcpy()s resp->len bytes from a remote NFC-F device		

CVE-2026-80803	response into the NFC_SENSF_RES_MAXSIZE-byte target.sensf_res field without an upper-bound check. A nearby malicious NFC-F device can send an oversized SENSF_RES response to overflow the stack-local struct nfc_target. Clamp resp->len to NFC_SENSF_RES_MAXSIZE before the copy. Found by 0sec automated security-research tooling (https://0sec.ai).	N/A	More Details
CVE-2026-80804	In the Linux kernel, the following vulnerability has been resolved: xfs: restore nofs context unconditionally in xfs_trans_roll When __xfs_trans_commit() fails in xfs_trans_roll(), the NOFS context is cleared but only restored in the success path. This leaves the error path without nofs protection, causing a circular lock dependency between xfs_nondir_ilock_class and fs_reclaim: CPU0 CPU1 ---- ---- lock(&xfs_nondir_ilock_class); lock(fs_reclaim); lock(&xfs_nondir_ilock_class); lock(fs_reclaim); Fix this by moving xfs_trans_set_context() before the error check so that nofs context is always restored on the new transaction.	N/A	More Details
CVE-2026-80806	In the Linux kernel, the following vulnerability has been resolved: ext4: don't enable DAX on new encrypted files Currently, when a new encrypted regular file is created, the call to ext4_set_inode_flags(inode, init=true) in __ext4_new_inode() is made before EXT4_INODE_ENCRYPT is set. As a result, it can set S_DAX if the filesystem is mounted with "-o dax=always". EXT4_INODE_ENCRYPT then actually gets set a bit later in __ext4_new_inode(), when it calls fscrypt_set_context() which calls ext4_set_context(). ext4_set_context() sets EXT4_INODE_ENCRYPT and calls ext4_set_inode_flags(inode, init=false) to set S_ENCRYPTED too. This was intended to clear S_DAX as well. However, this was broken by commit 043546e46dc7 ("fs/ext4: Only change S_DAX on inode load"). This causes data written to the file to bypass encryption, also causing xfstests failures such as generic/548 (when "-o dax=always" is used). Fix this by simplifying the flow by making __ext4_new_inode() set EXT4_INODE_ENCRYPT earlier. This makes it take effect in ext4_set_inode_flags(inode, init=true), making S_DAX never be set. Similarly, make EXT4_STATE_MAY_INLINE_DATA never be set in the first place on new encrypted inodes. Then it doesn't need to be cleared. As a result of these simplifications, ext4_set_context() no longer needs to change inode flags or state when 'handle != NULL'. Remove that too.	N/A	More Details
CVE-2026-80807	In the Linux kernel, the following vulnerability has been resolved: nilfs2: reject invalid block index in GC ioctl Syzbot reported list corruption caused by a double list_add_tail() call on bh->b_assoc_buffers within nilfs_lookup_dirty_data_buffers(). Analysis revealed that the root cause was the insertion of a page/folio with a page index of ULONG_MAX into the page cache via the GC ioctl. filemap_get_folios_tag(), called by nilfs_lookup_dirty_data_buffers(), repeatedly detects a dirty folio with a page index of ULONG_MAX due to index wrap-around, leading to duplicate processing of dirty buffers. As a preparatory step, the GC ioctl loads the page/folio of the block to be moved during GC and inserts it into the page cache based on information in the nilfs_vdesc structure passed as an argument. Normally, this does not cause issues because the user-space GC library configures the nilfs_vdesc structure properly. However, since there is no range check on the parameters determining the page index, a request with artificially crafted parameters -- such as those generated by Syzbot -- can result in a page/folio being inserted with a page index of ULONG_MAX, triggering the above problem. This resolves the issue by checking the ranges of 'vd_offset' and 'vd_vblocknr' in the nilfs_vdesc structure that determine the page index, thereby preventing the invalid page/folio insertions.	N/A	More Details
CVE-2026-80808	In the Linux kernel, the following vulnerability has been resolved: ext4: stop retrying saturated xattr cache entries ext4_xattr_block_set() retries when a cache entry selected for reuse has a saturated reference count after taking the buffer lock. The retry returns to the mbcache lookup without making that entry ineligible, so it can select the same unusable entry indefinitely. A task spinning there can hold the parent directory's i_rwsem and leave concurrent rmdir callers blocked. Normally a reusable entry has a reference count below EXT4_XATTR_REFCOUNT_MAX because the count and MBE_REUSABLE_B are updated under the same buffer lock. A corrupted filesystem can violate that invariant. The syzbot reproducer reports allocator and xattr corruption before triggering this retry loop. Check the untrusted on-disk count before incrementing it, avoiding overflow, and clear MBE_REUSABLE_B when it is already saturated. The next lookup then skips the entry that was just proven unusable. This mirrors the normal transition at EXT4_XATTR_REFCOUNT_MAX; the release path marks the entry reusable again on the exact 1024-to-1023 transition. Using the same QEMU harness and guest parameters, current unpatched Linux hung in 6 of 8 420-second trials with the do_rmdir signature; representative NMI backtraces caught the owner spinning in ext4_xattr_block_set(). The patched kernel completed 28 of 28 trials without a hung-task report; the final twelve trials exercised the reviewed overflow-safe form of the change. syzbot's patch testing also completed without reproducing the hang.	N/A	More Details
CVE-2026-80788	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: Do not WARN on remotely-controlled oversized SGL allocations When fuzzing the nvme target code, I tripped a kernel warning in nvmet_tcp_map_data() because the length passed into the allocator is controlled by the remote initiator. A remote initiator that sends a command with an SGL claiming a huge number, can create a scatterlist and iovec allocation of over 1 million entries, which causes the backing kmalloc call to exceed MAX_PAGE_ORDER and then the page allocator will trip on a WARN_ON_ONCE_GFP() message: WARNING: mm/page_alloc.c:5280 __alloc_frozen_pages_noprof Workqueue: nvmet_tcp_wq nvmet_tcp_io_work ... sgl_alloc_order nvmet_tcp_map_data nvmet_tcp_try_recv_pdu As it's never good to trip a kernel warning remotely due to many systems having panic-on-warn enabled, let's silence it by just add GFP_NOWARN to the allocation flags.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nvmet: pci-epf: fix use-after-free in nvmet_pci_epf_exec_iod_work() nvmet_pci_epf_exec_iod_work() submits an I/O command with req->execute() and then waits for the command to complete and transfers the data back to the host. This wait is		

CVE-2026-80787	not needed for commands that do not transfer data from the device to the host. To decide whether that wait is needed, it reads iod->data_len and iod->dma_dir after calling req->execute(). However, once req->execute() is called, the command may complete asynchronously on another CPU. For commands that do not require a device-to-host data transfer, nvmet_pci_epf_queue_response() calls nvmet_pci_epf_complete_iod() directly, which can free the iod before it reads iod->data_len and iod->dma_dir, resulting in the KFENCE use-after- free: BUG: KFENCE: use-after-free read in nvmet_pci_epf_exec_iod_work+0x288/0x798 [nvmet_pci_epf] Use-after-free read at 0x00000000fdfa6d03 (in kfence-#63): nvmet_pci_epf_exec_iod_work+0x288/0x798 [nvmet_pci_epf] process_one_work+0x15c/0x4f0 worker_thread+0x18c/0x30c kthread+0x130/0x140 ret_from_fork+0x10/0x20 kfence-#63: 0x00000000e3de0e71-0x00000000c938ad62, size=712, cache=kmalloc-1k allocated by task 10 on cpu 0 at 73.995480s (0.005122s ago): mempool_kmalloc+0x1c/0x28 mempool_alloc_noprof+0x40/0x9c nvmet_pci_epf_poll_sqs_work+0xd4/0x344 [nvmet_pci_epf] process_one_work+0x15c/0x4f0 worker_thread+0x18c/0x30c kthread+0x130/0x140 ret_from_fork+0x10/0x20 freed by task 131 on cpu 3 at 73.995521s (0.008385s ago): mempool_kfree+0x10/0x20 mempool_free+0x44/0x64 nvmet_pci_epf_free_iod+0x88/0x98 [nvmet_pci_epf] nvmet_pci_epf_cq_work+0xfc/0x280 [nvmet_pci_epf] process_one_work+0x15c/0x4f0 worker_thread+0x18c/0x30c kthread+0x130/0x140 ret_from_fork+0x10/0x20 Fix this by referring to iod->data_len and iod->dma_dir before calling req->execute(). The remaining iod accesses such as iod->status are only reached on the device-to-host read path. In this case, nvmet_pci_epf_queue_response() signals iod->done instead of freeing the iod, so the iod stays valid.	N/A	More Details
CVE-2026-80786	In the Linux kernel, the following vulnerability has been resolved: fbdev: Wrap user-invoked calls to fb_set_var() in helper Handle fbcon during display updates in fb_set_var_from_user(). Check with fbcon if the mode change is possible, update hardware state and finally update fbcon. Update all callers. Only the FBIOPUT_VSCREENINFO ioctl currently does all steps. Other mode-changes callers in sysfs and driver code are missing fbcon-related steps. With the new helper, ps3fb and sh_mobile_lcdcfb no longer maintain fbcon state themselves.	N/A	More Details
CVE-2026-80775	In the Linux kernel, the following vulnerability has been resolved: futex: Fix race on the initial mm->futex.phash.ref allocation futex_hash_allocate() allocates mm->futex.phash.ref without any locking. Commit d9b05321e21e ("futex: Move futex_hash_free() back to __mmput()") moved the allocation here and assumed that the process has just a single thread at this point. Commit ee9dce44362b ("futex: Drop CLONE_THREAD requirement for private default hash alloc") widened need_futex_hash_allocate_default() to cover any CLONE_VM clone, but left out vfork because the parent is suspended and cannot race. That no longer holds once vfork is nested. If a vfork child calls vfork again and is then killed with SIGKILL, the parent is released from its vfork wait and runs concurrently with the grandchild in the same mm. Neither of them went through futex_hash_allocate_default(). When both call prctl(PR_FUTEX_HASH, PR_FUTEX_HASH_SET_SLOTS) at the same time, each one sees mm->futex.phash.ref as NULL and stores its own percpu counter. Only the last store survives. The counter stored first is no longer reachable from the mm, so the references on it are not seen by __futex_ref_atomic_end(). A private hash that still has references is then considered dead and freed, and a task that still holds one of its buckets writes into freed memory in futex_q_lock(). Store the counter once with cmpxchg() and let the loser free_percpu() its own. The initial reference has to be taken before the store, otherwise another task can install a private hash while the counter is still 0.	N/A	More Details
CVE-2026-80767	In the Linux kernel, the following vulnerability has been resolved: HID: sensor: custom: Fix use-after-free in enable_sensor enable_sensor_store() can call set_power_report_state(), which dereferences sensor_inst->power_state and sensor_inst->report_state. These pointers refer to entries in sensor_inst->fields. Create the field attributes before exposing the enable_sensor sysfs attribute, so enable_sensor cannot be accessed before the state it depends on has been initialized. On remove, delete enable_sensor before freeing the field attributes, so a concurrent sysfs write cannot dereference freed memory through power_state or report_state.	N/A	More Details
CVE-2026-80768	In the Linux kernel, the following vulnerability has been resolved: HID: ft260: fix stack-use-after-return write in I2C read race ft260_i2c_read() points dev->read_buf at a caller-supplied buffer (often an on-stack variable), arms a completion and waits up to five seconds for the device to return the data. The HID input callback ft260_raw_event() runs in the input/IRQ path, independent of the dev->lock mutex held by the read path, and copies the device-supplied payload into dev->read_buf after a plain NULL check. These two paths share read_buf, read_idx and read_len with no serialization. If the device delays its response until the read times out, ft260_i2c_read() resets the controller, clears read_buf and returns, unwinding the stack frame the buffer lived in. A response that arrives at that moment lets ft260_raw_event() pass the NULL check and then memcpy() the device-controlled payload into the now-freed stack location, a bounded but attacker-influenced stack-use-after-return write triggerable by malicious or malfunctioning hardware. Add a dedicated spinlock that serializes every access to read_buf, read_idx and read_len. ft260_raw_event() now holds it across the NULL check, the memcpy and the index update, while the read path takes it when arming and when clearing the buffer, so the teardown can no longer slip between the check and the copy.	N/A	More Details
CVE-2026-80769	In the Linux kernel, the following vulnerability has been resolved: HID: rapoo: fix missing hid_is_usb() check to_usb_interface() can only be used on a hid_device whose parent is really USB; uhid can create devices that identify as being on BUS_USB, but don't actually have a USB parent. Fix the use of to_usb_interface() without a hid_is_usb() check. Add a dependency on USB_HID for hid_is_usb(), as other HID drivers do; the alternative	N/A	More Details

	would be to provide a simple stub implementation on !USB_HID builds. I have verified that it is currently possible to trigger a kernel splat due to this bug in an ASAN build, and that this commit fixes the issue.		
CVE-2026-80770	In the Linux kernel, the following vulnerability has been resolved: HID: nintendo: stop device IO before hid_hw_stop on probe failure nintendo_hid_probe() calls hid_device_io_start() before joycon_init() and joycon_leds_create(). If either fails, the error path jumps to err_close which calls hid_hw_close()/hid_hw_stop() without first calling hid_device_io_stop(). hid_hw_stop() does not stop device IO, so hid_input_report() may still run and access driver data that is being torn down, resulting in a use-after-free. Add an err_io_stop label that calls hid_device_io_stop() before hid_hw_close(), and point the two post-io_start error paths at it.	N/A	More Details
CVE-2026-80771	In the Linux kernel, the following vulnerability has been resolved: HID: nintendo: register input device after capabilities are set input_register_device() exposes the device to userspace immediately. In joycon_input_create() it was called before joycon_config_rumble() configures the FF_RUMBLE capability and the memless force-feedback device, so a concurrent EVIOCSFF could dereference a NULL dev->ff. Registering early also means the initial udev event lacks button and axis information, which can make input managers ignore the device. Move input_register_device() to the end of joycon_input_create(), after all capabilities, the IMU input device and the force-feedback callbacks have been configured.	N/A	More Details
CVE-2026-80772	In the Linux kernel, the following vulnerability has been resolved: HID: nintendo: fix out-of-bounds read in joycon_ctlr_read_handler() joycon_ctlr_read_handler() casts an incoming HID input report to struct joycon_input_report and parses it, guarding the cast only with a 12-byte length check: if (size >= 12) /* make sure it contains the input report */ joycon_parse_report(ctlr, (struct joycon_input_report *)data); struct joycon_input_report is 49 bytes: a 13-byte header followed by a union whose IMU arm is 36 bytes. For an IMU report joycon_parse_report() -> joycon_parse_imu_report() walks that union (struct offsets 13..48), so a report of exactly 12 bytes with data[0] == JC_INPUT_IMU_DATA passes the guard yet is read up to 37 bytes past its declared length. The over-read bytes are decoded into accelerometer/gyroscope values and forwarded to userspace through the "(IMU)" input device, leaking driver-internal memory. data[0] and size are fully controlled by a malicious or spoofed Joy-Con/Pro Controller. Receive buffers are sized to the maximum report length, so this is an over-read within the allocation rather than a slab OOB, but the decoded bytes still reach userspace. The sibling subcmd path in joycon_ctlr_handle_event() already bounds the same cast correctly: if (size < sizeof(struct joycon_input_report) || data[0] != JC_INPUT_SUBCMD_REPLY) break; Use the same sizeof(struct joycon_input_report) bound here.	N/A	More Details
CVE-2026-80773	In the Linux kernel, the following vulnerability has been resolved: HID: huawei: fix missing hid_is_usb() check to_usb_interface() can only be used on a hid_device whose parent is really USB; uhid can create devices that identify as being on BUS_USB, but don't actually have a USB parent. Fix the use of to_usb_interface() without a hid_is_usb() check. I have verified that it is currently possible to trigger a kernel splat due to this bug in an ASAN build, and that this commit fixes the issue.	N/A	More Details
CVE-2026-80774	In the Linux kernel, the following vulnerability has been resolved: HID: asus: fix missing hid_is_usb() check to_usb_interface() can only be used on a hid_device whose parent is really USB; uhid can create devices that identify as being on BUS_USB, but don't actually have a USB parent. Fix the use of to_usb_interface() without a hid_is_usb() check. I have verified that it is currently possible to trigger a kernel splat due to this bug in an ASAN build, and that this commit fixes the issue.	N/A	More Details
CVE-2026-80776	In the Linux kernel, the following vulnerability has been resolved: futex: Fix race in futex_pivot_pending() during private hash resize A task performing a custom private hash resize can remain blocked in uninterruptible sleep indefinitely. The hung-task detector reports: INFO: task futex-resizer:314 blocked for more than 10 seconds. task:futex-resizer state:D stack:14824 pid:314 tgid:312 ppid:311 Call Trace: __schedule+0x521/0xf30 schedule+0x22/0xa0 futex_hash_allocate+0x3db/0x490 __do_sys_prctl+0x6f5/0xbd0 do_syscall_64+0xf9/0x530 entry_SYSCALL_64_after_hwframe+0x77/0x7f Kernel panic - not syncing: hung_task: blocked tasks futex_pivot_pending() allows the resize request to continue when either no replacement hash is pending (hash_new == NULL) or the current hash reference count has reached zero. After the final-reference wake, another futex task can complete the pivot between the two observations: T1 T2 futex_hash_allocate() wait_var_event(mm, ...) futex_pivot_pending(mm) hash_new != NULL futex_hash() futex_ref_get(old) -> false futex_pivot_hash(mm) hash_new = NULL __futex_pivot_hash(mm, new) rcu_assign_pointer(hash, new) fph = rcu_dereference(hash) /* new */ futex_ref_is_dead(fph) -> false schedule() The pivot changes the state from hash_new != NULL with a dead current hash to hash_new == NULL with a live current hash. Because futex_pivot_pending() reads hash_new and hash without serialization, the resize task can observe hash_new in the pre-pivot state and hash in the post-pivot state, causing futex_pivot_pending() to return false even though the pivot has completed. The task then goes to sleep after the wakeup has already been consumed. Serialize state reads in futex_pivot_pending() using futex_mm_phash::lock. This guarantees that futex_pivot_pending() observes hash_new and hash atomically, eliminating the race condition.	N/A	More Details
CVE-2026-80785	In the Linux kernel, the following vulnerability has been resolved: fbdev: serialize mode sysfs access with lock_fb_info() show_mode(), show_modes(), and store_mode() access fb_info->modelist and fb_info->mode without holding lock_fb_info(). store_modes() takes lock_fb_info() while replacing the modelist and freeing the old one. A concurrent reader or writer can load a pointer to an old modelist entry before store_modes() frees it, then dereference freed memory or store a stale freed pointer in fb_info->mode. Take lock_fb_info() in show_mode(), show_modes(), and store_mode() to serialize with store_modes(). In show_mode(), copy the	N/A	More Details

	mode to the stack and format after dropping the lock. In store_mode(), split activate() into a _locked variant to avoid double-locking, and hold the locks for the modelist walk, mode conversion, activation, and fb_info->mode assignment together.		
CVE-2026-80777	In the Linux kernel, the following vulnerability has been resolved: futex/pi: Plug private futex exec() race The check for private futexes whether the waiter's mm, which is stored in the futex_key and copied into the pi_state, is the same as the owner's mm is not sufficient for exec(). exec() has a gap where the mm check fails to give the correct answer: exec() ... exec_release_mm() futex_exec_release() tsk::futex::exit_state = EXITING; cleanup_robust_list(); 1) tsk::futex::exit_state = OK; ... old_mm = tsk::mm; 2) tsk::mm = ->mm; Between #1 and #2 the check for the mm is wrong as that mm is about to be swapped out and eventually freed. Plug this gap by: 1) Setting tsk::futex::exit_state to FUTEX_STATE_DEAD in futex_exec_release() 2) Setting tsk::futex::exit_state to FUTEX_STATE_OK after the mm has been switched. From a futex point of view the task is dead after it finished the robust list cleanup up to the point where it sets the state to OK again.	N/A	More Details
CVE-2026-80778	In the Linux kernel, the following vulnerability has been resolved: futex/pi: Reject cross-mm private futex owners A private futex key borrows the waiter's mm without taking an mm_users reference. Nevertheless, attach_to_pi_owner() currently accepts an owner from a different address space and copies the private key into the owner's PI state. When that owner exits, exit_pi_state_list() uses the saved key to find the hash bucket and acquires a reference to the waiter's private hash. If the last user of the waiter's mm exits concurrently, futex_hash_free() frees the hash while the owner still uses its bucket and reference. Prevent this by validating in attach_to_pi_owner() that, for private futexes, the owner mm and waiter mm are the same. Perform the check with the owner's pi_lock held and after validating owner::futex::state to serialize against a concurrent PI-state exit cleanup. [tglx: Amended comment]	N/A	More Details
CVE-2026-80779	In the Linux kernel, the following vulnerability has been resolved: net/ionic: avoid OOB TX partner lookup for hwstamp RXQ The dedicated hardware timestamp RX queue is allocated with q->index equal to lif->ionic->nrxqs_per_lif. The normal txqcqs array only contains the regular queue pairs, so using that index to set rxq->partner can read one entry past txqcqs[] and then write through the derived pointer. Only link RX/TX partners for normal queue-pair indexes. Leave the hwstamp RX queue unpaired, and make the XDP_TX path abort cleanly if an RX queue has no TX partner.	N/A	More Details
CVE-2026-80780	In the Linux kernel, the following vulnerability has been resolved: HID: pidff: fix OOB write when hid->inputs is empty hid_pidff_init_with_quirks() derives its input_dev from list_entry(hid->inputs.next, struct hid_input, list) without first checking that hid->inputs is non-empty. The list member of struct hid_input is at offset 0, so on an empty list list_entry() yields &hid->inputs itself and the following hidinput->input load reads an unrelated member of struct hid_device. dev is then a type-confused pointer, and force-feedback init writes through it: each set_bit(FF_*, dev->ffbit) stores 8 bytes at dev + 192, past the end of the object dev actually aliases, and input_ff_create() adds further writes of a heap pointer and two function pointers. Until hid-universal-pidff the only caller was hid_pidff_init() from usbhid, which runs under HID_CLAIMED_INPUT and therefore always has at least one hid_input. universal_pidff_probe() starts the device with HID_CONNECT_DEFAULT & ~HID_CONNECT_FF and then calls hid_pidff_init_with_quirks() directly whenever the descriptor carries a PID usage page, bypassing that gate. A report descriptor whose only application collection is on HID_UP_PID leaves hid->inputs empty while hid_connect() still succeeds through the hidraw claim, so probe reaches the unguarded list_entry(). The write happens in the USB probe path, on the hotplug workqueue, so plugging in a malicious device is enough to trigger it; no attacker software and no logged-in user are required. KASAN reports an 8-byte out-of-bounds write in hid_pidff_init_with_quirks() reached from universal_pidff_probe(). Check for an empty list before deriving dev and return -ENODEV, as the other HID force-feedback drivers already do. universal_pidff_probe() propagates the error and unwinds. Discovered by XBOW, triaged by Baul Lee <baul.lee@xbow.com>	N/A	More Details
CVE-2026-80781	In the Linux kernel, the following vulnerability has been resolved: HID: core: fix OOB read of field->usage in hid_set_field() hid_set_field() hands field->usage + offset to hid_dump_input() before the guard that bounds offset: hid_dump_input(field->report->device, field->usage + offset, value); if (offset >= field->report_count) { hid_err(...); return -1; } Under CONFIG_DEBUG_FS hid_dump_input() dereferences that pointer, with buf = hid_resolv_usage(usage->hid, NULL). The usage[] array is allocated inline with the hid_field in hid_register_field() and holds field->maxusage entries, so an offset past it reads off the end of the kvzalloc()ed allocation and into a neighbouring object. Had the guard run first, offset < report_count <= maxusage would already have confined the pointer to the array. A caller supplies such an offset today. picolcd_fb_send_tile() validates only report->maxfield before issuing hid_set_field(report->field[0], 11 + i, ...) for i = 0..31, so its offsets are fixed at 11..42 and are never checked against the bound field. When the device registers that field with fewer usages, the framebuffer deferred-io work drives the read on every tile. KASAN reports a 4-byte slab-out-of-bounds read in hid_dump_input() below hid_set_field(), and the same boot logs "offset (1) exceeds report_count (1)" from the guard that runs only afterwards. Move the hid_dump_input() call below the guard. Because field->maxusage >= field->report_count, the guard then establishes that field->usage + offset lies inside the array before it is dereferenced, for every caller and without changing behaviour on the valid path. Discovered by XBOW, triaged by Baul Lee <baul.lee@xbow.com>	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: HID: magicmouse: do not keep a stale msc->input if no input is claimed magicmouse_input_mapping() caches the first hid_input's input_dev in msc->input while the report descriptor is parsed, and the rest of the driver treats a non-NULL msc->input as proof		

CVE-2026-80782	that an input device was registered. That does not hold on the hid-input error path. If hidinput_connect() fails -- for instance because input_register_device() returns an error -- it unwinds through hidinput_disconnect(), which frees every input_dev it created, including the one cached in msc->input. The failure does not abort the probe. hid_connect() only skips the claim: if ((connect_mask & HID_CONNECT_HIDINPUT) && !hidinput_connect(hdev, connect_mask & HID_CONNECT_HIDINPUT_FORCE)) hdev->claimed |= HID_CLAIMED_INPUT; and the "device has no listeners" bailout below it does not fire for this driver, which sets ->raw_event; on the USB Magic Mouse 2 / Magic Trackpad 2 paths hidraw and hiddev are claimed as well. hid_hw_start() therefore returns 0 and magicmouse_probe() continues with msc->input pointing at freed memory. Being non-NULL, it passes the "input not registered" check in probe and the NULL checks in ->raw_event and ->event, so the next input report dereferences freed memory. Clear msc->input when the HID core did not claim an input device, so the existing NULL checks cover this case as well.	N/A	More Details
CVE-2026-80783	In the Linux kernel, the following vulnerability has been resolved: HID: magicmouse: prevent unbounded recursion in magicmouse_raw_event() magicmouse_raw_event() handles DOUBLE_REPORT_ID (0xf7) packets, which pack two touch reports into one, by splitting the packet and calling itself on each half. The only guard against runaway recursion is a "size < 1" check, which stops zero-sized calls but does not bound the recursion depth. A malicious HID device that matches this driver can send a report starting with DOUBLE_REPORT_ID and filled with the sequence [0xf7, 0x00]. Each level consumes two bytes and recurses on the remainder, so an incoming report of up to HID_MAX_BUFFER_SIZE (16 KiB) drives roughly 8000 nested calls. That easily exhausts the 16 KiB kernel stack, leading to a stack overflow: a panic with CONFIG_VMAP_STACK, or memory corruption without it. A double report only ever wraps two normal reports; it is never legitimately nested. Refuse to re-enter the DOUBLE_REPORT_ID case from a recursive call so the recursion depth is bounded to two, while all valid packets keep being parsed exactly as before.	N/A	More Details
CVE-2026-80784	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: fix memory leak from alloc-during-teardown race mptcp_pm_destroy() empties msk->pm.anno_list and msk->pm.userspace_pm_local_addr_list under msk->pm.lock during socket teardown, dropping the lock between the two. A concurrent userspace PM genl ANNOUNCE on the same msk holds a sock reference via mptcp_token_get_sock() and, in mptcp_pm_nl_announce_doit(), calls mptcp_userspace_pm_append_new_local_addr() and mptcp_pm_announced_alloc(). Both take msk->pm.lock briefly to add to their respective lists. Because the genl handler holds a sock reference, mptcp_pm_destroy() may run on the same msk via mptcp_disconnect(), which invokes mptcp_destroy_common() without dropping the sock refcount, before the handler completes. If the lock acquisitions interleave such that mptcp_pm_destroy() empties a list first, the later alloc adds its entry to a list head that nothing else iterates for this msk, and the entry leaks. kmemleak reports both mptcp_pm_add_addr objects (from mptcp_pm_announced_alloc()) and mptcp_pm_addr_entry objects (from mptcp_userspace_pm_append_new_local_addr()) under sustained concurrent ANNOUNCE + close load against the userspace PM. Add an MPTCP_PM_DESTROYING bit in msk->pm.status, set by mptcp_pm_destroy() under pm.lock before the lists are emptied and checked under pm.lock by the alloc paths. Either the alloc takes pm.lock first, in which case its entry is on the list when mptcp_pm_destroy() frees it; or mptcp_pm_destroy() takes pm.lock first, in which case the later alloc observes the bit and refuses. Found by an MPTCP protocol-flow harness extending BRF (arXiv:2305.08782).	N/A	More Details
CVE-2026-15937	Improper certificate validation in Checkmk <2.5.0p10 allows a relay and a push agent that share the same UUID to reuse each other's mTLS certificate to authenticate against agent receiver endpoints in either direction, because the endpoints do not verify that the certificate was issued by their own root certificate.	N/A	More Details
CVE-2026-70403	XING CPTrans-ME-X contains a Use of Hard-coded Password (CWE-259). Anyone with the knowledge of the credential may log in to the affected device.	N/A	More Details
CVE-2026-69657	XING CPTrans-ME-X contains a Use of Default Password (CWE-1393). Anyone with the knowledge of the credential may log in to the affected device.	N/A	More Details
CVE-2026-66840	XING CPTrans-ME-X contains an Exposure of Sensitive System Information to an Unauthorized Control Sphere (CWE-497). Sensitive system information may be leaked.	N/A	More Details
CVE-2026-80728	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/amdgpu: fix aperture mapping leak" devres teardown is LIFO. The aperture devres node was registered after the DRM device node, so devres_release_all() unmaps the aperture before the DRM device release callback fires amdgpu_device_fini_sw(). IP sw_fini callbacks (e.g. vcn_v4_0_sw_fini) write to fw_shared through a pointer derived from aper_base_kaddr, causing a kernel page fault on probe failure / rollback: BUG: unable to handle page fault ... PMD 0 RIP: vcn_v4_0_sw_fini+0x7b/0x170 [amdgpu] Call Trace: amdgpu_device_fini_sw amdgpu_driver_release_kms devm_drm_dev_init_release devres_release_all This reverts commit d871e99879cb5fd1fa798b006b4888887e63a17a. (cherry picked from commit 336e0cd576817ac64a4b394ca2b3680029f3e37f)	N/A	More Details
CVE-	A CSV injection vulnerability exists in SYS600. Injected malicious formulas can add or modify data to the spreadsheet, insert links, exfiltrate data, and in some cases, depending on how the user has their		

2026-9852	environment configured, execute malicious code on the user's machine. To exploit this issue attackers would need a way to create arbitrary log messages. This could be achieved through normal functionality via SCIL scripts, a log injection vulnerability, or via the SYS600 broker. This vulnerability affects all Windows users regardless of their privilege level who can run the Notify service and export the log.	N/A	More Details
CVE-2026-9853	A vulnerability exists in SYS600 which allows any user authenticated to the operating system of the server hosting the application to read and modify application objects without being authenticated to the SYS600 system itself. Only the SYS600 system users should be permitted to view and modify application objects.	N/A	More Details
CVE-2026-9854	A vulnerability exists in SYS600 RBAC mechanism where users having access to the engineering tools could elevate their privileges to administrator level on the underlying Windows host, granting themselves full control over the host machine.	N/A	More Details
CVE-2026-80727	In the Linux kernel, the following vulnerability has been resolved: x86/mce: Set up the polling timer before CMCI discovery I hit the following on one of my machines: mce: CPU0 BANK15 CMCI inherited storm ----------[cut here]---------- ODEBUG: assert_init not available (active state 0) object: (____ptrval____) object type: timer_list hint: 0x0 WARNING: lib/debugobjects.c:632 at debug_object_assert_init+0x178/0x230, CPU#0: swapper/0/0 CPU: 0 UID: 0 PID: 0 Comm: swapper/0 Not tainted 7.2.0-rc5 #3 PREEMPTLAZY RIP: 0010:debug_object_assert_init+0x18f/0x230 Call Trace: <TASK> __mod_timer mce_timer_kick cmci_discover intel_init_cmci mce_intel_feature_init mcheck_cpu_init identify_cpu identify_boot_cpu arch_cpu_finalize_init start_kernel A second splat follows right after, from timer_setup() finding that same timer already queued: ODEBUG: init active (active state 0) object: (____ptrval____) object type: timer_list hint: stub_timer+0x0/0x10 This is happening because CMCI storm detection is trying to modify the timer before latter was properly set up. Set up the timer first. __mcheck_cpu_setup_timer() only calls timer_setup(), and depends on neither the generic nor the vendor init. [bp: Massage commit message.]	N/A	More Details
CVE-2026-6071	A remote code execution security issue exists in the affected products when parsing DOE files that could allow a remote attacker to write past the end of an allocated object and execute code within the context of the current process. To exploit this vulnerability, a legitimate user must visit a malicious page or open a malicious file.	N/A	More Details
CVE-2026-80515	In Eclipse Arrowhead versions from 5.0.0 to 5.2.1 the management-authorization gate that protects every /…/mgmt/… REST endpoint decides whether to apply its check by calling request.getRequestURL().toString().contains("/mgmt/"). Tomcat returns getRequestURL() un-decoded, while Spring MVC's DispatcherServlet routes on the decoded path. Requesting /serviceregistry/%6Dgmt/systems (%6D == m) therefore fails the substring check — the filter falls through without authorising — yet is decoded to /serviceregistry/mgmt/systems and dispatched to the management controller. Spring Security's StrictHttpFirewall (active via spring-boot-starter-security in arrowhead-common) only rejects encoded / \ . % ; and null bytes, so percent-encoded ASCII letters pass through. Any authenticated system — regardless of privilege — can reach every management operation, including POST /authentication/mgmt/identities which creates new sysop accounts, yielding full administrative takeover of the local cloud.	N/A	More Details
CVE-2026-82180	In Eclipse Arrowhead versions from 5.0.0 to 5.2.1 when the MQTT API is enabled with the certificate authentication policy, CertificateMqttFilter parses an X.509 certificate that the client sends inside the MQTT message payload (the authentication field of MqttRequestTemplate) and treats its Subject DN as the authenticated identity. The certificate is decoded with CertificateFactory.generateCertificate() but its signature is never verified and its issuer chain is never validated against any trust store. Authorisation is reduced to two string comparisons on attacker-supplied data: the DN-qualifier must equal "sy" or "op", and the cloud-name part of the CN must match the server's. Both values are public (the cloud name is in the server's own TLS certificate). An attacker who can publish to the MQTT broker can therefore mint a self-signed certificate with CN=Sysop.<cloud>.<org>.arrowhead.eu, dnQualifier=op, send it as the authentication field, and be authenticated as the cloud's system operator with isSysOp == true. This passes the downstream ManagementServiceMqttFilter (request.isSysOp() → allowed) and gives full management access over MQTT. The HTTP CertificateFilter is not affected — it reads the certificate from jakarta.servlet.request.X509Certificate, which Tomcat populates only after a successful mTLS handshake against the configured trust store.	N/A	More Details
CVE-2026-80254	Authorization bypass through user-controlled key issue exists in ShizenBox2 (edge-app). If exploited, an attacker who can log in to the product may change the other user's password.	N/A	More Details
CVE-2026-80253	An improper physical access control issue exists in ShizenBox2 (dev-conf). If exploited, an attacker with physical access to the product may execute bootloader commands without authentication.	N/A	More Details
CVE-2026-78304	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-78080	Joomla Extension - feenders.de - Unauthenticated SQL injection in JooDatabase Lite < 5.1.0 - The cid parameter is used in queries without validation, allowing SQLi vectors.	N/A	More Details

CVE-2026-78069	Joomla Extension - j2commerce.com - Missing authorization on Apps controller delegation chain in J2Store 1.0.0-3.3.21, 4.0.0-4.0.21, 4.1.0-4.1.6 - `J2StoreControllerApps`'s `appTask` delegation path instantiates app-plugin controllers with no ACL check anywhere in the code. It currently returns 403 only as a side effect of `fof.xml`'s wildcard-deny resolving under the singularised ACL key `app`, which has no explicit allow rule — not because of any deliberate check. Behind that path, `applocalizationdata::getInstallerTool()` used a caller-influenced table name with no allow-list, both to select a `#__j2store_*` table for truncation and to build a path to SQL files it then executes — a path-traversal-capable file read/execute.	N/A	More Details
CVE-2026-78065	Joomla Extension - j2commerce.com - Guest checkout address disclosure to any authenticated user (IDOR) in J2Store 1.0.0-3.3.21, 4.0.0-4.0.21, 4.1.0-4.1.6 - `editAddress()` redirected non-owners away only when the loaded address row had a **non-empty** `user_id` belonging to someone else. Guest-checkout address rows have an empty `user_id`, so that check never triggered for them — any logged-in account guessing a small, sequential `address_id` got a guest customer's full name, street address, and phone number rendered prefilled into the edit form.	N/A	More Details
CVE-2026-78064	Joomla Extension - j2commerce.com - Anonymous cart-record tampering via inherited FOF `save` task in J2Store 1.0.0-3.3.21, 4.0.0-4.0.21, 4.1.0-4.1.6 - `fof.xml` grants the `carts` view's tasks a wildcard `true` ACL, and FOF only enforces CSRF tokens on back-end HTML requests, not on front-end `format=raw` requests. `J2StoreControllerCarts` already scoped `remove()` to the caller's own session, but never overrode the generic FOF `save` task, so it remained reachable to insert new cart rows with an attacker-chosen `user_id`/`session_id`, or overwrite an existing row by id.	N/A	More Details
CVE-2026-78000	Joomla Extension - j2commerce.com - Reflected XSS via `filter_tag`, `pricefrom` and `priceto` in J2Store 1.0.0-3.3.21, 4.0.0-4.0.21, 4.1.0-4.1.6 - Four task handlers accepted a base64-encoded URL from user input and redirected to it without validating the destination host, enabling phishing using the shop's trusted domain. No authentication required.	N/A	More Details
CVE-2026-85199	Eclipse aeriOS Self-orchestrator versions prior to 1.2.1 contain a path traversal vulnerability in the REST API. User-controlled identifiers used to create, update, or delete Self-orchestrator resources were incorporated into filesystem paths without adequate validation or sanitization. An unauthenticated remote attacker able to access the Self-orchestrator API could therefore supply specially crafted identifiers containing path traversal sequences to write or delete JSON files outside the intended application directories, subject to the filesystem permissions of the Self-orchestrator process. The impact is increased by the absence of authentication on the affected API and by the container running with elevated privileges in the affected deployment configuration. The issue has been addressed in version 1.2.1 by introducing validation and sanitization of user-controlled identifiers before they are used to construct filesystem paths, preventing path separator characters from being used to escape the intended directories.	N/A	More Details
CVE-2026-77999	Joomla Extension - j2commerce.com - Unauthenticated PayPal callback forgery leading to order confirmation fraud in J2Store 1.0.0-3.3.21, 4.0.0-4.0.21, 4.1.0-4.1.6 - The PayPal IPN listener's signature check (`_validateIPN()`) accepted `UNVERIFIED` and any non-`INVALID` response as valid, made its verification request with `CURLOPT_SSL_VERIFYPEER` disabled, and stored its verdict in a field nothing downstream ever checked — so processing continued regardless of the outcome. Separately, the paid-amount comparison only ran when `mc_gross` was a positive number; omitting the field from the POST body (`floatval(null) == 0`) skipped the check entirely. Combined with a merchant-configured `receiver_email` and a sequential, enumerable order id read from the `custom` field, an anonymous POST was enough to move a pending order straight to `CONFIRMED` with no payment, or force another customer's pending order to `FAILED`. `paypalv2.php` performed no amount check under any circumstances.	N/A	More Details
CVE-2026-76178	A stored Cross-Site Scripting (XSS) vulnerability in the notification template functionality of the endpoint /ocsreports/?function=notification. A user with administrator privileges can input malicious HTML content which is subsequently stored and displayed without proper sanitisation when other administrators access the template customisation view, allowing JavaScript code to be executed within the application’s security context and potentially compromising the sessions of other users with administrative privileges.	N/A	More Details
CVE-2026-80729	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: initialise workingset state before folio split xas_try_split() adds __GFP_ACCOUNT for page-cache xa_nodes, but __folio_split() leaves the xa_state's xa_lru unset. That lets a live, memcg-charged xa_node exist without being linked into the mapping's shadow_nodes list_lru; when reclaim later walks the list_lru it trips VM_WARN_ON(!css_is_dying()). Use mapping_set_update() to install both the workingset update callback and the shadow_nodes list_lru on the xa_state.	N/A	More Details
CVE-2026-85173	n8n versions before 2.36.2 contain a missing per-project authorization vulnerability in the Insights API routes that allows authenticated users with insights scopes to access workflow names and execution statistics across projects. Attackers can supply arbitrary projectId parameters to retrieve sensitive project and workflow information from projects they have no membership in.	N/A	More Details
CVE-2026-85172	n8n versions before 2.34.1 contain a server-side request forgery vulnerability in the legacy request helper function exposed to Code and Function nodes. The validation logic checks the uri property for SSRF safety while the underlying HTTP client uses the url property when both are present, allowing attackers to bypass validation by supplying a safe uri alongside a malicious url to access internal addresses.	N/A	More Details

CVE-2026-84831	SEPPmail Secure Email Gateway before 15.0.7 creates a fully privileged session before required multi-factor authentication enrollment is completed. An attacker with the password for an MFA-required but unenrolled account can access protected functionality without providing a second factor.	N/A	More Details
CVE-2026-80743	In the Linux kernel, the following vulnerability has been resolved: ASoC: xilinx: formatter_pcm: pass aud_drv_data to irq handlers The irq handlers take a struct device pointer and call dev_get_drvdata() to obtain the driver data. However, the driver data is only set at the end of probe, after devm_request_irq(), so an interrupt taken in between causes the handlers to pass a NULL pointer to readl() and crash. Pass the private data directly as the devm_request_irq() argument instead of the device pointer, matching what the handlers expect.	N/A	More Details
CVE-2026-80742	In the Linux kernel, the following vulnerability has been resolved: af_packet: Don't send zero-byte data in tpacket_snd(). syzbot reported a WARNING in __dev_queue_xmit() triggered via tpacket_snd(): skb_assert_len WARNING: at include/linux/skbuff.h:2753 skb_assert_len WARNING: at __dev_queue_xmit+0x21bc/0x4970 net/core/dev.c:4781 Call Trace: <TASK> dev_queue_xmit include/linux/netdevice.h:3448 [inline] packet_xmit+0x243/0x310 net/packet/af_packet.c:276 tpacket_snd net/packet/af_packet.c:2907 [inline] packet_sendmsg+0x28d6/0x4eb0 net/packet/af_packet.c:3134 When sending 0-byte packets via TPACKET ring buffer on devices with no hard header (e.g. dev->hard_header_len == 0), tpacket_fill_skb() populates an skb with skb->len == 0 and returns 0. tpacket_snd() then forwards this empty skb to packet_xmit(), causing __dev_queue_xmit() to hit skb_assert_len(skb). Similar checks exist in packet_snd() via commit dc633700f00f ("net/af_packet: check len when min_header_len equals to 0") and in packet_sendmsg_spkt() via commit 6a341729fb31 ("af_packet: Don't send zero-byte data in packet_sendmsg_spkt()."). Return -EINVAL in tpacket_fill_skb() when skb->len is zero to reject zero-length packets in tpacket_snd().	N/A	More Details
CVE-2026-80740	In the Linux kernel, the following vulnerability has been resolved: drm/log: Fix infinite loop when scale is too large for display When scale is large enough that scaled_font exceeds the display dimensions, rows or columns become 0. A columns value of 0 causes an infinite loop in drm_log_draw_kmsg_record() because the loop never decrements len. Check for zero rows/columns in drm_log_setup_modeset() and return an error, cleaning up the already allocated buffer to avoid a leak.	N/A	More Details
CVE-2026-80739	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: TC, Check if flow is PEER before acquiring devcom lock In case __mlx5e_add_fdb_flow() fails in lower levels, the flow is deleted via mlx5e_tc_del_flow(), and mlx5e_tc_del_flow() is acquiring ESW devcom lock without condition. In addition, in case of peer_flow, __mlx5e_add_fdb_flow() is called while holding ESW devcom comp lock. This results in an AA deadlock. To fix this, introduce a new PEER flag that is set on flows created as peer flows (the duplicate flows on peer devices), and check it in mlx5e_tc_del_flow() before acquiring ESW devcom lock. Lockdep splat: == WARNING: possible recursive locking detected == Possible unsafe locking scenario: CPU0 ---- lock(&comp->lock_key#2); lock(&comp->lock_key#2); *** DEADLOCK *** Call Trace: <TASK> dump_stack_lvl+0x69/0xa0 print_deadlock_bug.cold+0xbd/0xca __lock_acquire+0x1671/0x2ec0 lock_acquire+0x10e/0x2e0 down_read+0x95/0x430 mlx5_devcom_for_each_peer_begin+0x4e/0xe0 [mlx5_core] mlx5e_tc_del_flow+0x11d/0xa70 [mlx5_core] mlx5e_flow_put+0x99/0x100 [mlx5_core] __mlx5e_add_fdb_flow+0x409/0xf00 [mlx5_core] mlx5e_configure_flower+0x2a86/0x4100 [mlx5_core] mlx5e_rep_setup_tc_cls_flower+0x12f/0x1b0 [mlx5_core] mlx5e_rep_setup_tc_cb+0x153/0x750 [mlx5_core] tc_setup_cb_add+0x1dc/0x470 fl_change+0x2f4d/0x626d [cls_flower] tc_new_tfilter+0x79b/0x2310 rtnetlink_rcv_msg+0x778/0xad0 do_syscall_64+0x70/0x960 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK>	N/A	More Details
CVE-2026-80755	In the Linux kernel, the following vulnerability has been resolved: selinux: reject a permission value exceeding the class permission count perm_read() bounds a permission value by SEL_VEC_MAX but never by the nprim of the owning class or common, which is taken verbatim from the policy image. security_get_permissions() then writes perms[value - 1] into an nprim-sized kcalloc() array, so a class declaring fewer permissions than its largest permission value drives an out-of-bounds heap write. The top-level symbol tables are validated this way; the nested per-class permission table is not. Reject a permission whose value exceeds nprim, which is already set when perm_read() runs. Well-formed policies are unaffected. [PM: tweak comment for line length]	N/A	More Details
CVE-2026-80756	In the Linux kernel, the following vulnerability has been resolved: selinux: do not cancel a policy conversion that never started sel_write_load() calls selinux_policy_cancel() when sel_make_policy_nodes() fails, and that helper dereferences the outgoing policy to cancel its sidtab conversion. On the first policy load there is no outgoing policy: security_load_policy() returns early for that case, before it converts anything, and state->policy is still NULL. A first load that fails while building the selinuxfs tree therefore takes a NULL dereference in selinux_policy_cancel(), reached from a write(2) to /sys/fs/selinux/load. Skip the cancel when there is no old policy, mirroring the check security_load_policy() already makes before it converts.	N/A	More Details
CVE-2026-80757	In the Linux kernel, the following vulnerability has been resolved: selinux: reject a class permission count below its inherited common security_get_permissions() maps an inherited common's permissions into an array sized by the class's own permissions.nprim, but class_read() takes that nprim verbatim from the policy image and never checks that it covers the common. A class that inherits a common of N permissions while declaring a smaller nprim is accepted, and on load the common's permissions are written past the class-sized array -- an out-of-bounds heap write. Reject a class whose permission count is below its inherited common's.	N/A	More Details

	Well-formed policies, where the class count already includes the inherited permissions, are unaffected.		
CVE-2026-84830	SEPPmail Secure Email Gateway before 15.0.7 contains a command injection vulnerability that allows authenticated administrators to execute commands with elevated privileges.	N/A	More Details
CVE-2026-84832	SEPPmail Secure Email Gateway before 15.0.6 deserializes attacker-controlled data in a privileged REST import workflow without adequate validation. An attacker with a privileged API token can execute arbitrary commands with "nobody" privileges.	N/A	More Details
CVE-2026-85171	n8n before 1.123.73, 2.35.4, and 2.36.2 contains a credential exposure vulnerability in the Strapi, SeaTable, and Mailcheck nodes. These nodes send their decrypted credentials to the authentication endpoint via the raw legacy HTTP helper outside any error handling, causing the plaintext secret to be persisted in execution error data. Any authenticated user can read the plaintext secret from their own execution through the REST API, bypassing the blank-value redaction enforced by the credentials API.	N/A	More Details
CVE-2026-80733	In the Linux kernel, the following vulnerability has been resolved: net: remove WARN_ON_ONCE() from sk_mc_loop() sk_mc_loop() can be called for sockets that are neither AF_INET nor AF_INET6 (e.g. AF_PACKET sockets when sending packets via raw/packet socket over virtual devices such as VRF or ipvlan). In such cases, sk_family is not AF_INET/AF_INET6 and sk_mc_loop() falls through the switch statement and triggers WARN_ON_ONCE(1). Non-INET sockets do not support IP_MULTICAST_LOOP or IPV6_MULTICAST_LOOP options, so loopback should default to true without generating a warning.	N/A	More Details
CVE-2026-80730	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Fix crash passing ERR_PTR to kthread_stop() In test_ringbuffer()'s out_free cleanup loop, the check `!rb_threads[cpu]` only catches NULL entries and misses entries that hold an ERR_PTR. rb_threads[] is static, so unassigned slots are NULL. But when kthread_run_on_cpu() fails for a cpu, it stores ERR_PTR(-ENOMEM) (or -EINTR) in rb_threads[cpu] before the creation loop jumps to out_free. That entry is non-NULL, so the old `!ptr` check does not break, and the cleanup proceeds to call kthread_stop() on the ERR_PTR. kthread_stop() then dereferences the bogus pointer, crashing the kernel during the late_initcall self-test. crash logs: BUG: kernel NULL pointer dereference, address: 000000000000001c Oops: 0002 [#1] SMP NOPTI CPU: 1 PID: 1 Comm: swapper/0 Not tainted 7.2.0-rc6-dirty #7 PREEMPT(lazy) RIP: 0010:kthread_stop+0x2e/0x220 RBX: fffffffffffffff4 CR2: 000000000000001c Call Trace: <TASK> test_ringbuffer+0x1ec/0x650 do_one_initcall+0x6c/0x2c0 kernel_init_freeable+0x21d/0x420 kernel_init+0x15/0x1c0 ret_from_fork+0x21b/0x320 </TASK> Kernel panic - not syncing: Fatal exception	N/A	More Details
CVE-2026-85165	n8n versions before 2.36.2 contain an expression sandbox bypass vulnerability where free identifiers in spread, computed-key, switch-case, or class-extension positions resolve against process globals. Authenticated users with workflow-edit permission can mutate host objects through expression evaluation, with changes persisting process-wide until restart.	N/A	More Details
CVE-2026-85166	n8n before 2.35.4 and 2.36.x before 2.36.2 does not validate credential references in the inline workflow JSON of nodes that execute an inline sub-workflow (e.g., the Workflow Tool node). A shared-workflow editor, or any user creating/updating a workflow via the REST API, Public API, or MCP, can persist a node referencing a credential they do not own. When the workflow is later executed under an identity that holds the credential, the inline sub-workflow resolves the secret and can send it to an attacker-controlled endpoint, resulting in credential exfiltration.	N/A	More Details
CVE-2026-85167	n8n before 2.35.4 and 2.36.x before 2.36.2 contain a query injection vulnerability in the Elasticsearch Document Get All and Google Cloud Firestore Document Query operations, which build their JSON query by interpolating expression values directly into the query string before parsing. A value containing quote and brace characters can close the intended field and introduce new query operators, turning an intended single-document lookup into a full-collection read.	N/A	More Details
CVE-2026-85168	n8n versions before 1.123.73, 2.35.4, and 2.36.2 contain a remote code execution vulnerability in the Git node. The node reset a fixed list of command-bearing configuration keys before each operation, but that list did not cover the content-filter and merge-driver key families. A repository with local configuration setting one of those keys together with a matching attribute pattern causes git to execute the configured command during an ordinary Add, Commit, Checkout, or Pull operation. The command runs as the n8n process user.	N/A	More Details
CVE-2026-85169	n8n versions before 1.123.73, 2.35.4, and 2.36.2 contain an expression sandbox escape in the $fromAI handler. $fromAI resolved a caller-supplied placeholder name without requiring it to be an own property and admitted reserved keys; against a primitive input value it returned a live host-prototype reference. An attacker with workflow-build privilege can walk the prototype chain to the Function constructor and compile/execute arbitrary code in the main n8n process, leading to remote code execution.	N/A	More Details
CVE-2026-85170	n8n versions before 1.123.73, 2.35.4, and 2.36.2 pass message content in the Gmail (v1) and Brevo nodes to the mail composer without verifying it is a string. An authenticated user able to run a workflow can supply an expression that resolves to an object carrying a path or href property, causing the composer to read a local file accessible to the n8n process or fetch an internal URL (SSRF) and attach the result to the outgoing message.	N/A	More Details
	Server-Side Request Forgery (SSRF) vulnerability in the /ocsreports/?function=tele_activate endpoint due to		

CVE-2026-76177	insufficient validation of the HTTPS_SERV and FILE_SERV parameters. An authenticated user with operator privileges can provide arbitrary values for these parameters, causing the OCS Inventory server to make HTTP/HTTPS requests to external systems or internal resources, which could allow access to internal network services or metadata resources of cloud services.	N/A	More Details
CVE-2026-76176	SQL injection vulnerability in the endpoint /ocsreports/index.php?function=admin_double due to improper processing of the values in the ID field included in the selected_grp_dupli[] parameter. An authenticated user with operator privileges can manipulate these values to alter the SQL queries executed by the application and retrieve information stored in the database.	N/A	More Details
CVE-2026-85216	MISP contains an authentication bypass vulnerability in its LDAP and LinOTP authentication components due to insufficient validation of user-supplied credentials. The custom LdapAuthenticate and LinOTPAuthenticate components replace CakePHP's FormAuthenticate implementation but did not replicate its credential validation checks. As a result, empty or non-string values could reach the underlying authentication mechanisms. In the LDAP authentication path, an attacker able to identify a valid directory user's email address could submit an empty password. The empty credential could be passed to ldap_bind(), where an LDAP server accepting unauthenticated binds may return a successful result for a valid distinguished name combined with an empty password. MISP could consequently treat the attacker as the corresponding authenticated directory user without verification of the user's password. The issue also affected the LinOTP authentication component. Invalid credential types were not rejected before being processed, and when mixed authentication was enabled, an empty password could be checked against a locally stored MISP password hash. LDAP-provisioned MISP accounts could additionally be created with an empty local password because account creation skipped normal validation, resulting in a hash corresponding to an empty password. This could permit authentication through the local fallback mechanism when such an account was no longer resolved through LDAP. Successful exploitation could allow a remote unauthenticated attacker to impersonate an existing MISP user. If the targeted account has administrative or other privileged permissions, the attacker could gain corresponding access to sensitive threat-intelligence data, modify or delete information, alter configuration, or perform other privileged operations. The patch resolves the vulnerability by requiring authentication identifiers and passwords to be valid strings, rejecting empty passwords where they are not explicitly permitted, and assigning a randomly generated local password to LDAP-provisioned accounts instead of storing a hash derived from an empty password.	N/A	More Details
CVE-2026-77121	A user account with permission to deploy artifacts to a hosted Maven repository could upload a POM file containing an oversized metadata field. This causes future attempts to list or browse that repository's components to permanently fail until an administrator repairs the underlying data. Only the targeted repository is affected; other repositories and overall server health remain unaffected.	N/A	More Details
CVE-2026-85063	node-csv is a full-featured CSV parser with a simple API that is tested against large datasets. Prior to 7.0.2, csv-parse with the columns and group_columns_by_name options enabled treats a duplicate __proto__ header as an existing property in packages/csv-parse/lib/api/index.js, assigns an attacker-controlled array through obj['__proto__'], and replaces the parsed record object's prototype. A malicious CSV header can therefore inject inherited array values into the returned record, hide those inherited values from JSON serialization, and affect property enumeration and type or shape checks in applications that process the record. This issue is fixed in version 7.0.2.	N/A	More Details
CVE-2026-85458	Divide-by-zero in Xpdf 4.06 (and earlier), when a glyph in a Type 3 font has a zero height.	N/A	More Details
CVE-2026-18167	A stack-based buffer overflow vulnerability exists in the EasyMesh module of TP-Link Archer AX55 v4. When Mesh mode is enabled, a LAN attacker may submit crafted input that causes the easymesh daemon to crash and may potentially achieve remote code execution on the device. Successful exploitation may cause the EasyMesh daemon to crash and may potentially allow remote code execution when Mesh mode is enabled. This may result in high impact to the confidentiality, integrity, and availability of the affected device.	N/A	More Details
CVE-2026-18330	A hard-coded cryptographic key vulnerability exists in the web module of TP-Link Archer AX55 v4. A LAN attacker who captures an HTTP login session may use the known shared RSA private key to decrypt the administrator password; the weakened AES session key further reduces the effort required to compromise session confidentiality. Successful exploitation may disclose the administrator password captured from an HTTP login session and compromise session confidentiality.	N/A	More Details
CVE-2026-77125	A vulnerability was identified in Sonatype Nexus Repository 3 in which two blobstore group management REST API endpoints did not correctly enforce the intended authorization check. A user granted only the nexus:blobstores:create permission could invoke these endpoints to convert an existing blobstore into a group blobstore, an action that should require the nexus:blobstores:update permission instead. This could result in unauthorized modification of blobstore configuration without administrator approval. The nexus:blobstores:create permission is a named permission that must be explicitly granted by an administrator; it is not held by default.	N/A	More Details
CVE-2026-	In affected versions of Nexus Repository 3, the script execution endpoint (POST /service/rest/v1/script/{name}/run) did not verify whether script execution had been administratively disabled. An account holding script-execution permission could continue to run previously-created scripts	N/A	More

77124	even after an administrator set nexus.scripts.allowCreation=false, undermining the expectation that this setting fully blocks script execution.		Details
CVE-2026-77123	Nexus Repository 3 contains a sensitive information disclosure vulnerability in the capability read API. An account holding the nexus:capabilities:read privilege can retrieve the plaintext shared secret configured on a webhook capability, which is intended to be masked from all API responses. This issue affects Nexus Repository 3 versions 3.2.0 through 3.95.x, and is fixed in version 3.96.0.	N/A	More Details
CVE-2026-77122	An authorization flaw in the REST API repository details endpoint (GET /service/rest/v1/repositories/{repositoryName}) in Sonatype Nexus Repository 3 allowed an account holding read or browse permission on a group repository to retrieve metadata for member repositories on which it held no direct permission, by requesting the endpoint directly for the member repository name. For proxy repositories, the disclosed metadata includes the configured remote URL, which may reveal internal upstream hostnames. This includes the anonymous user if it has been granted this permission; whether the anonymous user holds this permission depends on the role and permission configuration of the specific installation.	N/A	More Details
CVE-2026-53706	PREVAIL is a Polynomial-Runtime EBPF Verifier using an Abstract Interpretation Layer. Prior to version 0.2.4, the prevail eBPF verifier accepts ALU32 ADD and SUB instructions that operate on pointer-typed registers without checking the is64 flag. Because ALU32 arithmetic zero-extends the 32-bit result, the upper half of any pointer is silently destroyed at runtime, yet prevail marks the program as verified safe. Any caller that can submit an eBPF program for verification — including unprivileged users on kernels that permit BPF program loading — can produce a program that passes verification but faults or misbehaves at runtime. This issue has been patched in version 0.2.4.	N/A	More Details
CVE-2026-84452	Windows ML CLI is a command line tool for building portable, performant, and high-quality AI models for Windows ML. Prior to 0.4.0, the src/winml/modelkit/serve/cli_api.py component exposes WinML CLI commands through a localhost HTTP API without authentication and configures the allow_origins setting as a wildcard in both src/winml/modelkit/serve/cli_api.py and src/winml/modelkit/serve/app.py. A malicious website loaded by a user can send cross-origin requests to /v1/cli/build or /v1/cli/config and set the trust_remote_code parameter to true, which is converted to the --trust-remote-code command-line flag without validation. This reaches AutoConfig.from_pretrained with trust_remote_code=True in src/winml/modelkit/loader/_autoconfig.py and imports Python code from an attacker-controlled model repository, resulting in arbitrary code execution as the server user. This issue is fixed in version 0.4.0.	N/A	More Details
CVE-2026-53671	PREVAIL is a Polynomial-Runtime EBPF Verifier using an Abstract Interpretation Layer. Prior to version 0.2.4, the abstract transformer in prevail treats writes through a T_CTX-typed base register as a silent no-op: do_mem_store in src/crab/ebpf_transformer.cpp only models T_STACK stores, and the checker's T_CTX bounds arm never tests AccessType::write. An attacker can craft an eBPF program that overwrites a context field (e.g., ctx->data), reload that field typed as T_PACKET, and dereference an attacker-controlled address — and prevail will report the program as safe. This issue has been patched in version 0.2.4.	N/A	More Details
CVE-2026-53670	PREVAIL is a Polynomial-Runtime EBPF Verifier using an Abstract Interpretation Layer. Prior to version 0.2.4, in the Prevail eBPF verifier, EbpfTransformer::add() silently skips offset-variable updates when the destination register carries a non-singleton typeset (two or more simultaneously possible pointer types). Subsequent bounds checks use the stale offset and accept out-of-bounds memory accesses, so a crafted BPF program passes verification even though it would corrupt memory at runtime. This issue has been patched in version 0.2.4.	N/A	More Details
CVE-2026-67397	Path traversal in Plesk 18.0.79.9 and earlier and 18.0.80 through 18.0.80.5 allows local users to execute arbitrary code as root.	N/A	More Details
CVE-2026-67398	Missing authorization vulnerability has been discovered in 2Checkout payment gateway of WHMCS from 8.13.0 before 8.13.8, from 9.0.0 before 9.0.8, all other EOL versions from 4.5.0. The vulnerability allows an unauthenticated user to get WHMCS customer's data via 2Checkout payment gateway's endpoint under specific conditions.	N/A	More Details
CVE-2026-67402	An insecure Apache configuration in ConfigServer Security & Firewall maps /usr/bin as CGI programs through the Messenger v3 HTTPS virtual host. A remote unauthenticated attacker whose address is blocked can request a mapped executable and run arbitrary commands as the Apache user. The vulnerability affects installations where CSF Messenger v3 and its HTTPS mode are enabled. WebPros addressed the vulnerability in version 16.31.	N/A	More Details
CVE-2026-75754	Missing Authentication for Critical Function, Server-Side Request Forgery (SSRF), and Use of Hard-coded Credentials in ASUS Control Center allow an unauthorized user to obtain the encryption key via an HTTP request, causing a local service to enable SSH on port 2222. The attacker can then log in with the hardcode credentials to obtain a root shell, enabling direct reading, writing, and deletion of data on ASUS Control Center, as well as remote control of all servers, PCs, and workstations within the company. Refer to the 'Security Update for ASUS Control Center' section on the ASUS Security Advisory for more information.	N/A	More Details

CVE-2026-49249	Boruta is a standalone authorization server that aims to implement OAuth 2.0 and Openid Connect up to decentralized identity specifications. Prior to version 0.10.0, BorutaIdentityWeb.UserSettingsController.update/2 atomizes every key of the user-supplied request body via String.to_atom/1 before any validation. Because String.to_atom interns atoms permanently in the BEAM atom table (default cap 1,048,576 atoms; ERL_MAX_ATOMS), any authenticated end user can send PUT /users/settings with a user[<fresh-key>]=... body containing fresh keys per request and exhaust the global VM atom table. Once the table is full, the BEAM aborts with no more index entries in atom_tab and the entire OIDC server (auth, admin, gateway apps in the umbrella) crashes. The route is protected only by require_authenticated_user and a per-IP rate limit of 10 requests/second; a logged-in end user can hit it. The keys are atomized unconditionally before the downstream Accounts.update_user/6 call, so even failing updates contribute to exhaustion. This issue has been patched in version 0.10.0.	N/A	More Details
CVE-2026-62928	XING CPTrans-ME-X contains an OS Command Injection (CWE-78). Unauthenticated OS command may be injected.	N/A	More Details
CVE-2026-85062	Colord is a tiny yet powerful tool for high-performance color manipulations and conversions. Prior to 2.9.4, synchronous CSS color string matchers in src/colorModels/rgbString.ts, src/colorModels/hslString.ts, src/colorModels/hwbString.ts, src/colorModels/lchString.ts, and src/colorModels/cmykString.ts use the ambiguous numeric regular expression ([+-]?\d*.?\d+), allowing the same digits to be divided between overlapping quantifiers in quadratically many ways when malformed input is rejected. An attacker who can supply an unbounded color string to colord(), getFormat(), isEqual(), mix(), or contrast(), including through a request body, JSON field, or uploaded stylesheet, can block the processing thread with a multi-kilobyte payload. The affected matchers are parseRgbaString, parseHslaString, parseHwbaString, parseLchaString, and parseCmykaString. This issue is fixed in version 2.9.4.	N/A	More Details
CVE-2026-66048	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-85221	MISP contains an improper TLS certificate validation vulnerability in CurlClient. The CurlClient::$verifyPeer property was not explicitly initialized and therefore defaulted to null. When passed to cURL, this value effectively disabled TLS peer verification unless the calling code explicitly enabled it. As a result, HTTPS connections made through affected CurlClient instances could accept certificates that were not issued by a trusted certificate authority. An attacker capable of intercepting or manipulating network traffic between a MISP instance and a remote HTTPS service could impersonate the remote endpoint and perform a man-in-the-middle attack. Successful exploitation could allow an attacker to observe sensitive information transmitted by MISP, including authentication material or exchanged threat intelligence, and to modify responses returned to the MISP instance. The impact depends on the functionality using CurlClient and the data exchanged with the remote service. The patch enables TLS peer verification by default while preserving explicit support for configured self-signed certificates. It also corrects the self-signed certificate handling in SyncTool so that peer verification is disabled only when no pinned CA certificate is configured.	N/A	More Details
CVE-2026-75036	A security vulnerability was discovered in Fleet's Helm template preprocessing where templates evaluated by the Fleet controller could reach network resources outside the management cluster. A user who can supply bundle content to a repository referenced by a `GitRepo` resource can cause the Fleet controller to: - Disclose cluster metadata available to the templating context. - Reveal information about hosts reachable from the controller's network position. Because the disclosure channel is name resolution, it may remain effective in environments where outbound traffic is otherwise restricted. The disclosed information is limited to values exposed to the Fleet templating context and to name resolution results. Integrity and availability of managed clusters are not affected. This issue affects Fleet: from 0.12.0 before 0.12.19, from 0.13.0 before 0.13.15, from 0.14.0 before 0.14.10, from 0.15.0 before 0.15.6, and from 0.16.0 before 0.16.1.	N/A	More Details
CVE-2026-85226	MISP contains an authorization flaw in the OnDemand correlation engine where correlations were calculated solely from matching attribute values without applying the distribution, sharing group, organization, or other access-control restrictions associated with the correlated attributes and events. As a result, an authenticated user could receive correlation results referring to attributes or events that the user was not authorized to access. The vulnerable correlation collection path did not take the requesting user into account. The patch changes the correlation collector to accept the current user and filters the resulting attribute identifiers through MISP's existing fetchAttributesSimple() authorization logic, which evaluates event-, attribute-, object-, distribution-, and sharing-group-level restrictions against the live data. The issue also affected paths relying on previously stored correlation data. Because the OnDemand engine does not maintain the stored correlation table, its denormalized access-control information could be stale. The patch therefore validates correlated attribute identifiers against the current ACLs before returning them and additionally applies normal event visibility conditions when retrieving related events. An authenticated low-privileged user could exploit this issue by querying or creating attributes that correlate with restricted MISP content, potentially learning information about otherwise inaccessible events or attributes.	N/A	More Details
	MISP contains a reflected Cross-Site Scripting (XSS) vulnerability in the event attribute filtering query builder. The taggedAttributes and galaxyAttachedAttributes URL parameters were inserted into the query-builder		

CVE-2026-85227	rules without HTML escaping before being serialized as JSON and embedded inside a <script> element. Because JsonTool::encode() uses JSON_UNESCAPED_SLASHES, an attacker-controlled value containing a closing </script> sequence could terminate the surrounding script element and inject arbitrary HTML or JavaScript. For example, a specially crafted viewEventAttributes URL could contain malicious content in one of the affected filter parameters. An attacker could exploit the vulnerability by convincing an authenticated MISP user to follow a crafted URL. Successful exploitation would execute attacker-controlled JavaScript in the security context of the MISP instance and with the privileges of the victim's authenticated browser session. This could allow access to information available to the victim, modification of data through authenticated requests, or other actions permitted by the victim's MISP permissions. The vulnerability is addressed by applying HTML escaping with h() to both scalar and array values before they are inserted into the DOM.	N/A	More Details
CVE-2026-85230	A persistent unsafe URL injection vulnerability exists in the MISP dashboard ButtonWidget configuration. Dashboard widget URLs were validated only when the widget was rendered and were not validated when the configuration was saved. As a result, an authenticated user able to modify dashboard widget settings could persist arbitrary URL values, including URLs using the javascript: scheme, through either of the dashboard settings persistence paths. A malicious javascript: URL stored in a dashboard button could potentially result in client-side script execution in the MISP security context if the value reached a rendering or navigation path without the existing runtime validation. Such execution could allow an attacker to perform actions with the privileges of the affected user or access information available to their MISP session. The practical exploitability of this issue is reduced by the fact that MISP already applied URL validation at render time, which neutralized known malicious values before they were presented to the user. The vulnerability therefore represents a persistence-layer validation gap and a defense-in-depth weakness rather than evidence of a direct bypass of the existing rendering protection. The patch introduces a canonical url schema type and validates dashboard widget configuration before it is persisted through either settings save mechanism. ButtonWidget URLs must now be strings resolving to an absolute path on the current MISP instance or a full URL with the same origin. Values using javascript:, external origins, malformed URL forms, and non-string values are rejected at save time.	N/A	More Details
CVE-2026-76175	SQL injection vulnerability in the del_check parameter of the /ocsreports/?function=save_query_list endpoint. Input provided by an authenticated user with operator privileges is incorporated into an SQL query without proper parameterisation or validation, allowing the query to be manipulated and information to be extracted from the database using SQL injection techniques.	N/A	More Details
CVE-2026-53720	pymonocypher uses cython to wrap the Monocypher C library. Prior to version 4.0.2.8, the argon2i_32 implementation does not check the nb_blocks size. If the caller does not provide a sufficiently large buffer based on the API contract, then argon2i_32 will write past the end of the buffer and possibly corrupt the heap. This issue has been patched in version 4.0.2.8.	N/A	More Details
CVE-2026-53924	Gardens v2 is a modular governance framework that enables communities to create and manage multiple governance pools with customizable parameters and voting mechanisms. Prior to 0xc9d4e0dacd937364793278180551e59d93cd43f9, StreamingEscrow.claim() correctly rejects withdrawals while an escrow is disputed, but the permissionless syncOutflow() path performs the same excess-balance transfer without checking disputed. After a streaming proposal is challenged, anyone can call syncOutflow() to transfer escrowed SuperTokens to the proposal beneficiary while the dispute is pending. If the proposal is later rejected, those tokens cannot be recovered by drainToStrategy(). This issue has been patched in 0xc9d4e0dacd937364793278180551e59d93cd43f9.	N/A	More Details
CVE-2026-76174	Unrestricted file upload vulnerability in the CSV file upload functionality of the Ocsreports admin_info endpoint. The application validates files solely based on the name provided by the client, without properly checking their content or securely restricting the permitted file types. This allows a user with administrator privileges to upload PHP files to a directory accessible via the web interface. If the file is subsequently processed by the server, an attacker could execute arbitrary code with the privileges of the account used by the web service.	N/A	More Details
CVE-2026-57445	Gardens v2 is a modular governance framework that enables communities to create and manage multiple governance pools with customizable parameters and voting mechanisms. In dfba919e218e20d52db9f7b2e8d292d45a46c91b and prior, normal beneficiary payout paths in StreamingEscrow preserve depositAmount() while an active stream needs an escrow reserve. However, the approve-side dispute resolution path drains the whole available escrow balance to the proposal beneficiary. At time of publication, there are no publicly known patches.	N/A	More Details
CVE-2026-85236	A cross-site request forgery (CSRF) vulnerability existed in the cullEmptyEvents action of MISP. The endpoint performed a state-changing and irreversible operation while accepting HTTP GET requests. Because bodyless GET requests are not subject to CakePHP's CSRF validation, an attacker could cause an authenticated MISP user with sufficient privileges to invoke the endpoint simply by causing their browser to load a crafted URL, for example through an embedded image or other automatically requested resource. Successful exploitation triggers the deletion of published empty events. The deletion is particularly significant because the operation uses skipBlocklist, meaning the removed events do not leave blocklist entries that could prevent or track their subsequent synchronization. This can result in unintended and potentially irreversible deletion of MISP event records without explicit user interaction. The vulnerability was addressed by restricting cullEmptyEvents to HTTP POST requests, ensuring that CakePHP's normal CSRF protections are applied to the	N/A	More Details

	operation.		
CVE-2026-66049	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-85237	A vulnerability in MISP's email-based one-time password (OTP) authentication flow allowed an attacker to perform an unrestricted number of OTP verification attempts. The email_otp() endpoint did not apply brute-force protection when validating submitted OTP values. An attacker who had reached the OTP verification stage, for example after successfully providing a user's primary authentication credentials, could repeatedly submit candidate OTP values while the same OTP remained valid. This significantly increased the feasibility of guessing the OTP and bypassing the additional authentication factor, potentially resulting in unauthorized access to the affected user's account. The issue was exacerbated by the fact that the OTP is associated with the user rather than with an individual pending login session, allowing multiple concurrent sessions to attempt guesses against the same valid OTP. The patch integrates the existing MISP brute-force protection mechanism into the email OTP flow. Failed OTP attempts are now counted against the user, further attempts are rejected once the configured threshold is reached, and the active OTP is invalidated when the attempt budget is exhausted. Blocklisted users are also prevented from requesting the generation of a fresh OTP. In addition, OTP comparison now uses hash_equals() and validates that the submitted value is a string.	N/A	More Details
CVE-2026-85238	MISP contains a session fixation vulnerability in the CustomAuth authentication (a custom configuration) flow. When a user was successfully authenticated through CustomAuth, MISP stored the authenticated user identity in the existing session without first rotating the session identifier. As a result, if an attacker can cause a victim to use a session identifier known to the attacker before authentication, that same session identifier remains valid after the victim successfully authenticates. The attacker could subsequently reuse the fixed session identifier to access the victim's authenticated MISP session, potentially gaining the privileges associated with the victim's account. The issue occurs because __customAuthentication() wrote the authenticated user into the existing CakePHP session while the call to Session->renew() had previously been disabled. The patch restores session identifier rotation when a new authentication occurs or when the authenticated user changes, while avoiding unnecessary session renewal on every request.	N/A	More Details
CVE-2026-85239	A vulnerability in MISP's event template handling allowed an authenticated user with permission to create or modify event templates to bypass validation of the template definition field. The EventTemplate::beforeValidate() method only performed semantic validation when the supplied definition was already represented as an array. If a caller instead supplied a pre-encoded string, including malformed JSON or JSON representing an unexpected data type, the value bypassed validateDefinition() and only needed to satisfy the generic notBlank validation rule. As a result, an invalid event template definition could be stored persistently in the database. When event templates were subsequently retrieved, EventTemplate::afterFind() attempted to decode the stored definition using JsonTool::decode() without handling decoding failures. A definition containing invalid JSON could therefore trigger an exception during retrieval. Because the event template index is available to all authenticated users, a single malicious or malformed template could make the event template listing and other functionality relying on EventTemplate queries return HTTP 500 errors until the offending database row was manually repaired. Valid JSON representing an unexpected type, rather than the expected JSON object, could similarly result in invalid data reaching downstream consumers. The vulnerability can therefore be exploited by a user capable of saving event templates to persist malformed template data and cause a persistent denial of service against event-template functionality for other users. The patch enforces that event template definitions must be supplied as structured objects before saving and always applies semantic validation. On retrieval, malformed JSON and definitions that do not decode to the expected structure are caught, logged, and replaced with an empty definition, preventing a malformed database entry from breaking all event template queries. Poisoning doesn't seem reachable according to the lead developer.	N/A	More Details
CVE-2026-84736	In the current development version of Eclipse aeriOS, for which no official release has yet been published, the Federator component disables TLS certificate validation for outbound HTTPS connections by default. When the TLS_CERTIFICATE_VALIDATION environment variable is unset or set to false, the component configures its HTTP transport to skip TLS certificate verification. As a result, an attacker able to intercept network communications between the Federator and external services could impersonate those services and intercept sensitive information transmitted over HTTPS, including OAuth client credentials and bearer tokens. The issue has been addressed by enabling TLS certificate validation by default. The TLS_CERTIFICATE_VALIDATION environment variable is now set to true in the default configuration provided by the Helm chart and Docker Compose deployment.	N/A	More Details
CVE-2026-85242	PlaywrightCapture contains a server-side request forgery (SSRF) vulnerability in its favicon retrieval functionality. When only_global_lookup is enabled, the application validates the initial favicon URL to prevent requests to localhost, loopback, or other non-public network addresses. However, redirects followed by aiohttp were not subjected to the same validation. An attacker able to influence the content of a page processed by PlaywrightCapture could specify a publicly reachable favicon URL that responds with an HTTP redirect to a local or otherwise restricted address, such as 127.0.0.1, localhost, or an internal network service. Because aiohttp automatically followed the redirect, the resulting request could bypass the application's local-address restrictions and cause the PlaywrightCapture host to issue HTTP requests to resources that should not be externally reachable. Depending on the services reachable from the	N/A	More Details

	PlaywrightCapture host and how retrieved favicon data is subsequently exposed or processed, this could be used to probe internal HTTP services or potentially obtain information from otherwise inaccessible endpoints. The patch introduces an aiohttp request middleware that applies the existing local-URL validation to every request in the redirect chain. Requests resolving to restricted/local destinations are rejected before they are issued.		
CVE-2026-15431	A potential security vulnerability has been identified in the HP Support Assistant for versions prior to 9.53.2.0. The vulnerability could potentially allow a local attacker to escalate privileges due to insufficient access controls.	N/A	More Details
CVE-2026-15933	OptimiDoc Server (On-Premise) stores credentials for external services in cleartext. An authenticated administrator can view previously configured service passwords, including SMTP, FTP (for scan delivery), Active Directory (for user list import), and SharePoint credentials, in cleartext via the web administration panel page source, allowing exposure of sensitive third-party authentication data. This issue was fixed in version 26.08	N/A	More Details
CVE-2026-15926	Rejected reason: Red Hat Product Security has determined that this CVE ID is not needed	N/A	More Details
CVE-2026-80809	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix missing metadata reservation for large xattrs [BUG] lsetxattr() panics the kernel when setting a large xattr value on a fragmented filesystem where the file already has an external xattr block. [CAUSE] ocfs2_calc_xattr_set_need() never reserves metadata blocks for a new xattr value's extent tree when the file already has an external xattr block. The not_found path leaves meta_add at zero, so meta_ac is NULL when ocfs2_xattr_extend_allocation() runs. A new value root has room for a single extent record. On a fragmented filesystem, the allocator cannot satisfy the xattr value in one contiguous run, so each non-contiguous run requires its own extent record. When the value root's extent list is full and meta_ac is NULL, ocfs2_add_clusters_in_btree() returns RESTART_META, and ocfs2_xattr_extend_allocation() hits BUG_ON(why == RESTART_META). [FIX] The case where no xattr block exists yet already calls ocfs2_extend_meta_needed(&def_xv.xv.xr_list) to reserve value tree metadata. Add the same reservation to the case where an xattr block already exists, making the two cases consistent. Replace the BUG_ON with a -ENOSPC return so that if RESTART_META is returned despite the reservation, the error propagates to userspace instead of panicking the kernel.	N/A	More Details
CVE-2026-80810	In the Linux kernel, the following vulnerability has been resolved: io_uring/rsrc: fix folio size overflow in io_vec_fill_bvec() io_vec_fill_bvec() computes the folio size with a plain int 1: unsigned long folio_size = 1 << imu->folio_shift; imu->folio_shift is unsigned int and comes from folio_shift() of the folio backing the registered buffer, so it can be 32 or more on a 64 bit kernel. Shifting int 1 that far is undefined, and on x86 and arm64 the count is taken modulo 32, so a shift of 34 yields 4 rather than 16G. Every other folio_shift shift in this file already uses 1UL. The result is that the segment estimate and the fill loop disagree. io_estimate_bvec_size() sizes the bvec array with the real shift: max_segs += (iov[i].iov_len >> shift) + 2; so a 1M iovec on a 16G folio is charged 2 segments, while io_vec_fill_bvec() then walks the same iovec in folio_size chunks of 4 bytes and writes res_bvec[bvec_idx] a quarter of a million times, past the end of the array it was given. src_bvec is advanced once per iteration as well, so imu->bvec is read past its end at the same time. validate_fixed_range() only checks that the range is inside the registered buffer and does not bound the segment count. Reaching it needs a folio with a shift of at least 32, which means a gigantic hugetlb page: 16G on arm64 with 64K pages, where CONT_PMD_SHIFT is 34 and hugetlb_add_hstate(CONT_PMD_SHIFT - PAGE_SHIFT) registers that size, and likewise on powerpc. x86_64 tops out at 1G, so a shift of 30, which still fits in int and is unaffected. Use 1UL, as the rest of the file does.	N/A	More Details
CVE-2026-80811	In the Linux kernel, the following vulnerability has been resolved: io_uring/cmd: fix iovec leak when the async cmd is not recycled An io_async_cmd carries an iovec array in ->vec.iovec, allocated when the vec has to grow and kept across recycling through ctx->cmd_cache. On two paths nothing frees it and io_clean_op()'s kfree(req->async_data) drops the io_async_cmd without it. io_req_uring_cleanup() clears the async data flags only when io_alloc_cache_put() succeeds, and the cache holds IO_ALLOC_CACHE_MAX == 128 entries, so once it is full the put fails and the vec is left behind. An NVMe passthrough workload gets there without doing anything unusual: nvme_uring_cmd_io() returns -EIOCBQUEUED, so the io_async_cmd stays attached for the lifetime of the command and the live object count tracks the queue depth. Above 128 the puts start failing. ->cleanup is the last chance to free an inherited vec, since io_req_uring_cleanup() returns early for an io-wq issued command and is not called at all for one completed without ever being issued. But io_clean_op() calls ->cleanup only if REQ_F_NEED_CLEANUP is set, and for uring_cmd that happens only where the vec has to grow, so a command reusing a large enough cached vec never sets it. io_rw_alloc_async() and io_msg_alloc_async() flag an inherited vec for exactly this reason; io_uring_cmd_prep() does not. Flag an inherited vec in io_uring_cmd_prep(), and free the vec when the cache put fails, as io_req_rw_cleanup() does. The leak is invisible under KASAN, where io_alloc_cache_vec_kasan() frees the vec unconditionally.	N/A	More Details
CVE-	PJSIP is a free and open source multimedia communication library written in C. Prior to commit c4a151a, a stack buffer overflow exists in the GnuTLS TLS backend when parsing the Subject Alternative Name extension of a peer certificate (tls_cert_get_info() in ssl_sock_gtls.c). Only GnuTLS builds are affected (--with-gnutls); OpenSSL and Apple SecureTransport/Network.framework builds are not affected. While extracting certificate information after a TLS handshake, an incorrect buffer-size value can cause an oversized SubjectAltName		More

2026-57163	entry to be written past the end of a fixed-size stack buffer. A network-positioned attacker presenting a crafted certificate — a malicious server to a connecting client, or a malicious client to a server that requests certificates — can trigger this during the TLS handshake, before any SIP-level authentication. Impact may range from unexpected application termination to control flow hijack/memory corruption. This issue has been patched via commit c4a151a.	N/A	Details
CVE-2026-80906	In the Linux kernel, the following vulnerability has been resolved: net: packet: fix wrong transport_header when sending VLAN-tagged frame In packet_parse_headers(), when processing a VLAN-tagged frame, skb_set_network_header() is called to advance network_header past the VLAN tag to the inner protocol header. skb_probe_transport_header() is then called with skb->protocol still set to the outer VLAN EtherType (e.g. ETH_P_8021Q), while nhoff (derived from skb_network_offset()) already points past the VLAN tag to the inner protocol header. In __skb_flow_dissect(), proto is initialized to ETH_P_8021Q and nhoff points past the VLAN tag. When the dissector hits case ETH_P_8021Q, it reads a struct vlan_hdr at nhoff via __skb_header_pointer(), but that offset contains the inner protocol header (e.g. an IP header). The bytes are misinterpreted as a VLAN header, yielding a garbage encapsulated EtherType that matches no known protocol. The dissector returns false, so skb_probe_transport_header() never calls skb_set_transport_header(), leaving transport_header at its uninitialized sentinel value (~0U). Move skb_probe_transport_header() to before skb_set_network_header(). At the time skb_probe_transport_header() is called, network_header still points to the VLAN header, so nhoff correctly points to the VLAN header. The flow dissector can then parse the VLAN header, extract the inner EtherType, and advance nhoff to the inner protocol header, allowing transport_header to be set correctly.	N/A	More Details
CVE-2026-80907	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix UVD dpb min size calculation for H264 This should use actual number of references from the decode message, instead of maximum derived from level. (cherry picked from commit 64b525edb7e7bdfcdc77883c5e413804e2396856)	N/A	More Details
CVE-2026-80908	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Reject UVD message with dimensions above 4096 Fixes potential overflow in DPB size calculations. (cherry picked from commit 05e1387d151f71569fbe122d2c89f9db0c21dc10)	N/A	More Details
CVE-2026-80909	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Reject UVD message with invalid number of h265 refs Same change as for h264, avoids overflow later when calculating min dpb size. (cherry picked from commit a4b0720e4f1601f97f59a2be9c1b4b94fa6527d5)	N/A	More Details
CVE-2026-80910	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: lpass-wsa-macro: Fix enum kcontrol accesses EAR SPKR PA Gain" and the four "WSA RX* Mux" controls are enumerated, but their get and put callbacks access the value through ucontrol->value.integer.value[0] (a long) instead of ucontrol->value.enumerated.item[0] (an unsigned int). This same pattern was fixed in the sibling drivers by commit bcfe5f76cc40 ("ASoC: codecs: rx-macro: fix accessing array out of bounds for enum type") and commit 0ea5eff7c606 ("ASoC: codecs: va-macro: fix accessing array out of bounds for enum type"), but wsa-macro was missed. On 64-bit kernels with CONFIG_SND_CTL_DEBUG this trips the elem value sanity check and every read of these controls fails with -EINVAL.	N/A	More Details
CVE-2026-80911	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: sof-audio: Fix error path in sof_widget_setup_unlocked() If either tplg_ops->dai_config or widget_kcontrol_setup fail during widget setup we would double decrement the use_count of the widget because the sof_widget_free_unlocked() would be called twice, similarly the core_put would be invoked twice as well. Since the use_count and core_put() is handled within the widget_free function we need to return without falling through the pipe_widget_free label. The fixes tag is picked to the last change around this part of the code which is adequately old enough for backporting purposes.	N/A	More Details
CVE-2026-80912	In the Linux kernel, the following vulnerability has been resolved: selinux: reject an unclaimed class value in security_get_classes() security_get_classes() sizes an array by p_classes.nprim and fills it at value - 1, so a class value the policy never defines leaves a NULL. sel_make_classes() passes every entry to sel_make_dir(), reaching the same d_alloc_name() dereference as the permission array. The class symbol table is allowed to be sparse (policydb_class_isvalid() exists to absorb that), but this getter builds its own array straight from the hash table and has no such predicate. Fail the lookup when a value went unclaimed instead of handing out the NULL. Conforming policies define every class they declare and are unaffected.	N/A	More Details
CVE-2026-80913	In the Linux kernel, the following vulnerability has been resolved: selinux: require every boolean value to be defined p_bools.nprim comes from the policy image independently of how many booleans follow it, and cond_index_bool() fills bool_val_to_struct[] at value - 1, so a count larger than the values present leaves NULL entries. Every user of that array then walks it by index and dereferences each entry: cond_evaluate_expr() on the access-vector path, security_get_bools() and security_get_bool_value() behind selinuxfs, and security_set_bools(). A sparse class value is absorbed by policydb_class_isvalid() and its siblings; booleans have no such predicate, and no consumer that could use one. Reject a boolean value that no boolean defines, once, where the array is built. Conforming policies define every boolean they declare and are unaffected.	N/A	More Details
CVE-2026-71620	File Upload vulnerability in Zhao-github ApiAdmin v.5.0.1 allows a remote attacker to execute arbitrary code via a crafted .php file	N/A	More Details

CVE-2026-78839	An arbitrary file upload vulnerability in AppNitro MachForm v30 allows attackers to execute arbitrary code via uploading a crafted .phar file.	N/A	More Details
CVE-2026-80744	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables_offload: suppress WARN_ON_ONCE for ENOMEM in abort path In nft_flow_rule_offload_abort(), WARN_ON_ONCE(err) is triggered on every error during rollback, including -ENOMEM. Memory allocation failures are expected under low-memory conditions and do not indicate a kernel bug. Trace for example: nft_flow_offload_chain() // FLOW_BLOCK_BIND nft_flow_block_chain() nft_chain_offload_cmd() nft_block_offload_cmd() ->ndo_setup_tc() nsim_setup_tc() flow_block_cb_setup_simple() flow_block_cb_alloc() // fails to -ENOMEM The warning was reproduced on the 5.10 stable kernel under memory pressure via fault injection, but the underlying bug exists in mainline as well, as demonstrated by the ENOMEM trace above. The following splat was triggered during nf_tables transaction processing: WARNING: CPU: 0 PID: 8567 at net/netfilter/nf_tables_offload.c:532 nft_flow_rule_offload_abort net/netfilter/nf_tables_offload.c:532 [inline] WARNING: CPU: 0 PID: 8567 at net/netfilter/nf_tables_offload.c:532 nft_flow_rule_offload_commit+0x971/0xcd0 net/netfilter/nf_tables_offload.c:591 Modules linked in: CPU: 0 PID: 8567 Comm: syz-executor.0 Not tainted 5.10.260-syzkaller #0 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.12.0-1 04/01/2014 RIP: 0010:nft_flow_rule_offload_abort net/netfilter/nf_tables_offload.c:532 [inline] RIP: 0010:nft_flow_rule_offload_commit+0x971/0xcd0 net/netfilter/nf_tables_offload.c:591 Call Trace: nf_tables_commit+0x3bd/0x4bd0 net/netfilter/nf_tables_api.c:8604 nfnetlink_rcv_batch+0xb1e/0x1f20 net/netfilter/nfnetlink.c:509 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:579 [inline] nfnetlink_rcv+0x3b3/0x420 net/netfilter/nfnetlink.c:597 netlink_unicast_kernel net/netlink/af_netlink.c:1314 [inline] netlink_unicast+0x6cd/0xa00 net/netfilter/af_netlink.c:1340 netlink_sendmsg+0x906/0xe10 net/netfilter/af_netlink.c:1919 sock_sendmsg_nosec net/socket.c:651 [inline] __sock_sendmsg+0x155/0x190 net/socket.c:663 ____sys_sendmsg+0x705/0x870 net/socket.c:2379 ___sys_sendmsg+0x100/0x170 net/socket.c:2433 __sys_sendmsg+0xe9/0x1c0 net/socket.c:2462 do_syscall_64+0x33/0x40 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x67/0xd1 Change the condition to WARN_ON_ONCE(err && err != -ENOMEM) so that warnings are only emitted for unexpected errors. This aligns with the common kernel practice of not warning on -ENOMEM. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2025-13398	Rejected reason: This CVE ID is a duplicate of CVE-2025-13542 and was never published. Both IDs were assigned to the same unauthenticated privilege escalation vulnerability in the DesignThemes LMS WordPress plugin. All CVE users should reference CVE-2025-13542 instead of this ID.	N/A	More Details
CVE-2024-7956	A vulnerability exists in the affected products that allows a threat actor to gain access to user’s projects. To exploit this vulnerability the threat actor must have basic user privileges. If exploited, the threat actor can modify and delete the project.	N/A	More Details
CVE-2026-53602	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. Prior to version 0.3.7, two related authorization gaps let a host that should no longer be trusted obtain a fresh, valid Nebula certificate, because nebula-mgmt does not re-evaluate revocation/authorization state at certificate issuance time — only at poll time. Firstly, the blocklist is not enforced at sign / re-enroll time. internal/api/enroll.go:128 calls caMgr.Sign(...) without consulting the blocklist. The blocklist is only checked in the poll path (internal/api/updates.go:57, fingerprintInBlocklist). The blocklist is keyed by certificate fingerprint (internal/store/sqlite.go), so a re-enrollment produces a new fingerprint that is not in the blocklist. Secondly, renewal does not re-validate operator / CA status. Auto-renewal at poll time (internal/api/updates.go:285-319, signHostCert) reads host.Name, host.Groups, host.NebulaIPs from the DB and re-signs without checking whether the owning operator is still active or the CA still valid. DisableOperator (internal/store/sqlite_operators.go) revokes sessions and API keys but does not retire the operator's CAs, and pki/signer.go checks only CA cert time-expiry, not operator/CA status. This issue has been patched in version 0.3.7.	N/A	More Details
CVE-2026-53603	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. Prior to version 0.3.8, Operator session tokens are stored in plaintext in the operator_sessions table (the token column is the PRIMARY KEY). The session token is a 32-byte random hex value sent directly in a cookie and valid for 24 hours. Anyone who can read the database (backup, snapshot, file copy, or SQL-level disclosure) obtains every active session token and can hijack operator sessions directly, with no further authentication. This issue has been patched in version 0.3.8.	N/A	More Details
CVE-2026-53604	nebula-mesh is a self-hosted control plane for Slack Nebula mesh VPN. Prior to version 0.3.8, the web handler renderMobileBundle passes the real *pki.CAResolver directly into mobilebundle.Build. Inside Build, resolver.LoadByID decrypts the CA's ed25519 private key into a *pki.CAManager, but Build never calls CAManager.Wipe() on any return path. As a result, when a mobile-bundle request goes through the web UI and Build returns — especially on error (missing network, invalid prefix, DB error, signing failure) — the plaintext CA private key remains on the Go heap, unwiped, until garbage collection. An attacker able to read process memory (core dump, swap, memory-scraping) can recover the CA signing key, which would allow minting arbitrary host certificates for the mesh. The API handler already does this correctly: it loads the CAManager, defer caMgr.Wipe(), and wraps it in caManagerResolver. Only the web path is affected. This issue has been patched in version 0.3.8.	N/A	More Details

CVE-2026-71622	SQL injection vulnerability in Zhao-github APiAdmin v.5.0.1 allows a remote attacker to obtain sensitive information via the User.php component	N/A	More Details
CVE-2026-71625	An issue in slimkit plus ThinkSNS+ v.2.4 allows a remote attacker to escalate privileges via the ResetPasswordController.php component	N/A	More Details
CVE-2026-79389	Trueview T18161 S 6.0.23.4 contains an improper verification in MQTT command processing. An attacker with network access can replay or modify captured MQTT messages, including security-related nonce, timestamp, and signature fields, and the device accepts the modified messages and executes the associated commands.	N/A	More Details
CVE-2026-80905	In the Linux kernel, the following vulnerability has been resolved: net: tap: fix wrong transport_header when sending VLAN-tagged frame In tap_get_user_xdp(), when processing a VLAN-tagged frame (e.g. ETH_P_8021Q), skb_set_network_header() is called first to advance network_header past the VLAN tag to the inner protocol header. skb_probe_transport_header() is then called with skb->protocol still set to ETH_P_8021Q, while nhoff (derived from skb_network_offset()) already points past the VLAN tag to the inner protocol header. In __skb_flow_dissect(), proto is initialized to ETH_P_8021Q and nhoff points past the VLAN tag. When the dissector hits case ETH_P_8021Q, it reads a struct vlan_hdr at the current nhoff via __skb_header_pointer(), but that offset contains the inner protocol header (e.g. an IP header). The bytes are misinterpreted as a VLAN header, yielding a garbage encapsulated EtherType that matches no known protocol. The dissector returns false, so skb_probe_transport_header() never calls skb_set_transport_header(), leaving transport_header at its uninitialized sentinel value (~0U). Move skb_set_network_header() to after skb_probe_transport_header(). At the time skb_probe_transport_header() is called, network_header still points to the VLAN header (offset ETH_HLEN), so nhoff is correct and the flow dissector can parse the VLAN header, extract the inner EtherType, and advance nhoff to the inner protocol header, allowing transport_header to be set correctly.	N/A	More Details
CVE-2026-80904	In the Linux kernel, the following vulnerability has been resolved: net/tls: Fail tls_sw_splice_read() after a failed async decrypt When an async decrypt fails, tls_decrypt_done() records the error in ctx->async_wait.err and calls tls_err_abort(), which stores it in sk_err. tls_sw_recvmsg() and tls_sw_read_sock() each read async_wait.err once they hold the reader lock and fail the call: a record that did not authenticate breaks the connection. tls_sw_splice_read() has no such check, and sk_err does not stand in for one. tls_rx_rec_wait() tests sk_err only inside the loop it skips whenever a record is already parsed, and the first reader to reach sock_error() clears it, while async_wait.err persists. A splice therefore keeps delivering records on a connection that recvmsg() and read_sock() refuse to read. Read async_wait.err in tls_sw_splice_read() as the other two readers do.	N/A	More Details
CVE-2026-80903	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Fix sync entry leak on OA config emit failure xe_oa_emit_oa_config() releases the sync entries and the syncs array only on its success path. When it fails before the point of no return (fence allocation, config buffer allocation or batch submission), it returns without touching stream->syncs. The stream open path handles such failures in the caller, but xe_oa_config_locked() propagates the error without any cleanup, so the syncs array and the fence references held by the parsed entries are leaked. The next config ioctl overwrites stream->syncs, making the memory unreachable for good. Clean up the parsed syncs when xe_oa_emit_oa_config() fails, matching the cleanup done by the stream open error path. (cherry picked from commit 8af97b3da2cfce04e6b457c6eb17ed3c1daf912b)	N/A	More Details
CVE-2026-80892	In the Linux kernel, the following vulnerability has been resolved: erofs: cap LZMA stream pool size fs/erofs/decompressor_lzma.c sizes the module-global MicroLZMA stream pool from num_possible_cpus() when the lzma_streams module parameter is unset, then z_erofs_load_lzma_config() preallocates one image-supplied dictionary per stream, accepting dictionaries up to 8 MiB. On high-CPU systems, a small EROFS image can pin hundreds of MiB of vmalloc-backed decoder state until the erofs module is unloaded. Impact: An EROFS image mounted by the system can pin up to 8 MiB of vmalloc memory per LZMA stream, either as intended or unexpectedly. Bound the default stream count by a new CONFIG_EROFS_FS_ZIP_LZMA_DEFAULT_MAX_STREAMS option, default 16, so the worst-case default preallocation is 128 MiB if the number of CPUs is no less than 16 while preserving the existing per-image dictionary limit. An explicit lzma_streams module parameter is still honoured as-is, so administrators who deliberately size the pool are not affected.	N/A	More Details
CVE-2026-57165	PJSIP is a free and open source multimedia communication library written in C. Prior to commit 628b716, a stack buffer overflow exists in the PJLIB-UTIL telnet CLI front-end when redrawing the command line during history recall (handle_up_down() in cli_telnet.c). This affects only applications that enable the telnet CLI front-end (same gating as the related CLI issue). The line-redraw sequence for a recalled history entry can accumulate more data than a fixed-size stack buffer holds, which may lead to application termination. Exploitation requires access to the unauthenticated telnet CLI, which already permits arbitrary CLI commands, so the additional impact is limited. Applications that do not enable the telnet CLI front-end are not affected. This issue has been patched via commit 628b716.	N/A	More Details
	PJSIP is a free and open source multimedia communication library written in C. Prior to commit 4472a31, a		

CVE-2026-57166	stack buffer overflow exists in the PJLIB-UTIL telnet CLI front-end when rendering feedback for an entered command line. Several command-line handling paths write an attacker-influenced amount of data into fixed-size buffers without sufficient bounds checking, so a long command line can overflow them. This affects only applications that enable the telnet CLI front-end (e.g. pj_cli_telnet_create() / --cli-telnet-port). The telnet CLI is an interactive administration interface with no authentication, so any client able to reach it can already issue arbitrary CLI commands. A malformed or overly long command line can overflow a fixed-size stack buffer while rendering command-line feedback, which may lead to application termination. Because reaching this code already requires access to the unauthenticated CLI, the impact beyond that existing access is limited. Applications that do not enable the telnet CLI front-end are not affected. This issue has been patched via commit 4472a31.	N/A	More Details
CVE-2026-73848	Emlog is an open source website building system. In versions 2.6.29 and prior, tag names in emlog are not HTML-encoded when rendered in the article editor. An attacker can create a tag containing ');alert(document.domain);//. The addslashes() function does not escape HTML entities, so ' is stored as-is. When the browser renders the page, it decodes ' back to a literal single quote before evaluating the JavaScript, breaking out of the string and executing arbitrary code. At time of publication, there are no publicly known patches.	N/A	More Details
CVE-2026-80887	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: use check_add_overflow for shader size+offset bound vmw_shader_define() validates the user-supplied shader window against its backing buffer with (u64)buffer->tbo.base.size < (u64)size + (u64)offset drm_vmw_shader_create_arg::offset is __u64 in the uapi; when it is near U64_MAX the unsigned addition wraps and the resulting tiny value passes the check. The unbounded offset is then stored in res->guest_memory_offset and forwarded to host SVGA shader-create commands. Use check_add_overflow() to detect the wrap and compare the resulting endpoint against the buffer size.	N/A	More Details
CVE-2026-80888	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: drop dma_buf reference on foreign-fd prime import ttm_prime_fd_to_handle() returns -ENOSYS when the imported fd's dma_buf->ops do not match the ttm_object_device's ops, but does so without releasing the reference acquired by dma_buf_get(). Any unprivileged renderD client passing a non-vmwgfx prime fd through the DRM_VMW_GB_SURFACE_REF{,_EXT} path leaks one dma_buf reference per call and indefinitely pins the foreign exporter's GEM resources. Funnel the error path through the existing dma_buf_put() so the reference is always dropped.	N/A	More Details
CVE-2026-80889	In the Linux kernel, the following vulnerability has been resolved: can: isotp: fix timer drain order, wakeup handling and tx_gen ordering This patch is a follow-up to commit cf070fe33bfb ("can: isotp: serialize TX state transitions under so->rx_lock") which addresses following sashiko-bot findings: - isotp_sendmsg(): drain so->txfrtimer first so a stale callback can't re-arm echotimer after the claim - isotp_release(): wake so->wait after forcing ISOTP_SHUTDOWN so a sleeping sendmsg() claim isn't stranded - isotp_sendmsg(): have both wait_event_interruptible() calls in isotp_sendmsg() also wake on ISOTP_SHUTDOWN and do not return claim to IDLE to avoid corrupting a concurrent isotp_release() process. - isotp_sendmsg(): handle potential claim of a new transfer when the wait_event_interruptible() call returns in CAN_ISOTP_WAIT_TX_DONE mode. Don't touch timers and states of the new transfer if a new thread incremented so->tx_gen before getting the lock at err_event_drop. - isotp_sendmsg(): handle a stuck can_send() and omit timer and state changes if a new transfer was claimed. wait_tx_done() returns the error recorded in so->tx_result[], tagged with the caller's own generation. - isotp_tx_timeout(): on a claimed timeout, record the ECOMM error for the timed-out transfer's own generation in so->tx_result[]; sk->sk_err is raised unconditionally, same as every other error path here. - isotp_tx_gen_done()/isotp_tx_timeout(): always read tx.state (acquire) before tx_gen - the reverse order let a weakly ordered CPU pair a fresh tx.state with a stale tx_gen/tx_result slot. - isotp_sendmsg(): wait_tx_done: drain sk_err via sock_error() once we have read the result from so->tx_result[], so an already-reported error doesn't stay latched for a later poll()/SO_ERROR. Also align the remaining lock-free so->tx.state/rx.state/cfecho accesses and use skb->hash as unique loopback echo frame indicator.	N/A	More Details
CVE-2026-80890	In the Linux kernel, the following vulnerability has been resolved: sctp: reject stale cookies with mismatched verification tags sctp_unpack_cookie() skips cookie expiration checks whenever an association already exists. This is broader than the exception in RFC 9260 Section 5.2.4. For an existing association, Section 5.2.4 permits an expired State Cookie only when both Verification Tags in the cookie match the current association. Otherwise, the packet SHOULD be discarded and a Stale Cookie ERROR MUST be sent. The broad check lets an expired Action A restart cookie reach sctp_sf_do_dupcook_a(). In a runtime test with the default 60 second cookie lifetime, replaying such a cookie after 65 seconds returned a COOKIE-ACK and restarted the association. Check cookie expiration unless both Verification Tags match. This preserves the Action D exception for a lost COOKIE ACK while rejecting expired cookies in all other cases.	N/A	More Details
CVE-2026-80891	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: pci: Validate AIBV and AISB before pinning guest pages The AIBV holds one bit per MSI-X vector for a given function. The size of the bit vector is derived from the NOI and the AIBVO. If the size of the AIBV exceeds a single page boundary, then reject the request as we cannot safely pin the guest AIBV. Similarly reject the request if the AISB address is not 8-byte aligned as the architecture requires doubleword alignment for the summary bit address. Since the AISBO can address up to 64 bits, the size of the AISB can only be 8 bytes for the function. This also ensures the AISB doesn't exceed a single page boundary.	N/A	More Details

CVE-2026-80893	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix swap entry corruption when clearing uffd-wp at fork() copy_hugetlb_page_range() clears the uffd-wp bit of migration and hwpoison entries with huge_pte_clear_uffd_wp(), which operates on the present-PTE bit position. Swap entries keep the uffd-wp state elsewhere -- the migration branch reads and sets it with pte_swp_uffd_wp() and pte_swp_mkuffd_wp() -- and the present-PTE position falls into the swap payload. On x86-64 it lands in the inverted swap offset, where a naturally-aligned hugetlb PFN always has the affected bit set, so the clear advances the encoded PFN by two pages. No userfaultfd needs to be involved: the clear is guarded only by the child VMA not being uffd-wp registered, so a plain fork() with an in-flight hugetlb migration entry (or a poisoned hugetlb page) corrupts the entry copied into the child. Instrumenting the clear and forking after MADV_HWPOISON on a 2MB anon hugetlb page shows: offset before=120e00 offset after =120e02 The fallout is mostly latent: rmap walks match migration entries by folio range and remove_migration_pte() rebuilds the PTE from the folio, so a within-folio PFN skew heals once migration completes. But any path that re-encodes the corrupted offset -- e.g. hugetlb_change_protection() rewriting a writable migration entry via make_readable_migration_entry(swp_offset(entry)) -- propagates it. Migration entries legitimately carry uffd-wp, so clear it with pte_swp_clear_uffd_wp(), matching copy_nonpresent_pte() and move_huge_pte(). A hwpoison entry, on the other hand, never carries the uffd-wp bit: it is installed fresh by make_hwpoison_entry() (try_to_unmap_one() does not preserve uffd-wp on the hwpoison path) and hugetlb_change_protection() leaves hwpoison entries untouched. There was nothing to clear there, only the corruption, so drop the clear entirely.	N/A	More Details
CVE-2026-80902	In the Linux kernel, the following vulnerability has been resolved: dmaengine: sun6i-dma: Fix reclaim descriptors while terminating DMA When terminating DMA transfers, active descriptors are not properly reclaimed. Only cyclic descriptors were handled, leaving non-cyclic descriptors and their LLI chains to be permanently leaked. Fix by using vchan_terminate_vdesc() which handles both cyclic and non-cyclic descriptors by adding them to desc_terminated queue for proper cleanup. Add pchan->desc != pchan->done check to prevent double-adding completed descriptors, which would corrupt the list.	N/A	More Details
CVE-2026-80894	In the Linux kernel, the following vulnerability has been resolved: iommufd: Fix wrong hwpt passed to iommufd_auto_response_faults on replace iommufd_hwpt_replace_device() calls: iommufd_auto_response_faults(hwpt, old_handle); passing the *new* hwpt together with the handle of the device's *old* domain. This should be a parameter mismatch: 1. Semantically, iommufd_auto_response_faults(x, handle) scans x->fault's deliver list and response xarray for groups matching "handle". A group is queued under the hwpt that was attached at fault-delivery time. old_handle is fetched *before* the domain switch, so its group lives on old->fault, not on the new hwpt->fault. 2. Historically, the first argument was "old". The routine was introduced by commit b7d8833677ba ("iommufd: Fault-capable hwpt attach/detach/replace") as __fault_domain_replace_dev() in fault.c, correctly calling iommufd_auto_response_faults(old, curr). Commit fb21b1568ada ("iommufd: Make attach_handle generic than fault specific") moved this into iommufd_hwpt_replace_device() in device.c and swapped it to "hwpt". This should be a refactor regression, not an intentional change. Fix this by passing "old" instead.	N/A	More Details
CVE-2026-80895	In the Linux kernel, the following vulnerability has been resolved: mshv: Order pt_vp_array publish against irqfd assertion path mshv_partition_ioctl_create_vp() initialises a VP struct (allocations, mutex_init, init_waitqueue_head, page mappings) and then publishes the pointer into partition->pt_vp_array. Several ISR paths read this array locklessly: the intercept ISR, the two scheduler ISRs, and mshv_try_assert_irq_fast() on the irqfd fast path. Of these, only mshv_try_assert_irq_fast() can structurally race the publish. It runs from an eventfd waker without holding pt_mutex, and MSHV_IRQFD does not require the target lapic_apic_id (== vp_index) to refer to an existing VP at registration time. A user can therefore register an irqfd targeting a yet-to-be-created VP, then trigger mshv_try_assert_irq_fast() concurrently with MSHV_CREATE_VP for the same index. On weakly-ordered architectures the reader can observe a non-NULL pointer in pt_vp_array before the initialising stores to the VP struct become visible, leading to use of partially-initialised fields (e.g. vp_register_page). The other ISR readers cannot reach this race: the hypervisor will not generate intercept or scheduler messages for a VP that has never been told to run, and the user can only call MSHV_RUN_VP on the VP fd returned by MSHV_CREATE_VP, which by construction is returned after the publish. Leave those readers as plain loads. Use smp_store_release() in mshv_partition_ioctl_create_vp() to publish the pointer, and pair it with smp_load_acquire() in mshv_try_assert_irq_fast(). On x86 these compile to plain accesses under TSO; on ARM64 they emit one-instruction acquire/release barriers, acceptable on this fast path. The destroy-side path (destroy_partition() clearing pt_vp_array[i] to NULL after kfree(vp)) has a separate ordering and lifetime concern that is out of scope here.	N/A	More Details
CVE-2026-80896	In the Linux kernel, the following vulnerability has been resolved: mshv: Fix race in mshv_irqfd_deassign mshv_irqfd_deactivate() and the hlist traversal of pt_irqfds_list require pt->pt_irqfds_lock to be held, but mshv_irqfd_deassign() omits it. This races with the EPOLLHUP path in mshv_irqfd_wakeup(), which does take the lock before calling mshv_irqfd_deactivate(). Additionally, mshv_irqfd_deactivate() uses hlist_del() which poisons the node pointers rather than resetting them. Since mshv_irqfd_is_active() relies on hlist_unhashed() (checks pprev == NULL), a poisoned node still appears active. If a concurrent path calls mshv_irqfd_deactivate() again on the same irqfd, the guard fails to prevent a double hlist_del() on poisoned pointers. Fix both issues: - Add the missing spin_lock_irq/spin_unlock_irq around the list traversal in mshv_irqfd_deassign(), matching mshv_irqfd_release(). - Use hlist_del_init() instead of hlist_del() so the node is properly marked as unhashed after removal, making the is_active guard reliable.	N/A	More Details

CVE-2026-80897	In the Linux kernel, the following vulnerability has been resolved: netfs: release readahead folios on iterator preparation failure netfs_prepare_read_iterator() batches readahead folios in put_batch so that the folio references can be dropped after the I/O iterator has been prepared. If rolling_buffer_load_from_ra() fails after earlier folios have been batched, the function returns immediately and leaves those references held. Release the batch before returning the error.	N/A	More Details
CVE-2026-80898	In the Linux kernel, the following vulnerability has been resolved: netfs: clear PG_private_2 on copy-to-cache append failure netfs_pgpriv2_copy_to_cache() marks the folio with PG_private_2 before netfs_pgpriv2_copy_folio() appends it to the copy-to-cache rolling buffer. If the append fails, the folio is not queued for cache writeback, so the PG_private_2 state and its reference must be released immediately.	N/A	More Details
CVE-2026-80899	In the Linux kernel, the following vulnerability has been resolved: erofs: remove fscache backend entirely EROFS over fscache was introduced to provide image lazy pulling functionality. After the feature landed, the fscache subsystem made netfs a new hard dependency, which is unexpected for a local filesystem and has an kernel-defined caching hierarchy which could be inflexible compared to the fanotify pre-content hooks. Therefore, this feature has been deprecated for almost two years. As EROFS file-backed mounts and fanotify pre-content hooks both upstream for a while and already providing equivalent functionality (erofs-utils has supported fanotify pre-content hooks), let's remove the fscache backend now. The main application of this feature is Nydus [1], and they plan to move to use fanotify pre-content hooks in the near future too. I hope this patch can be merged into Linux 7.2, which is also motivated by newly found implementation issues [2][3] that are not worth investigating given the deprecation and limited development resources. The associated fscache/cachefiles cleanup patch will follow separately through the vfs tree (netfs) later: it seems fine since the codebase is isolated by CONFIG_CACHEFILES_ONDEMAND. [1] https://github.com/dragonflyoss/nydus/blob/v2.1.0/docs/nydus-fscache.md [2] https://github.com/dragonflyoss/nydus/pull/1824 [3] https://lore.kernel.org/r/20260619135800.1594811-1-michael.bommarito@gmail.com	N/A	More Details
CVE-2026-80900	In the Linux kernel, the following vulnerability has been resolved: ASoC: SDCA: Make UMP message size check more robust If message offset was larger than the buffer length the size check will pass incorrectly. Refactor the check such that it is more robust to invalid sizes.	N/A	More Details
CVE-2026-80901	In the Linux kernel, the following vulnerability has been resolved: ipvs: fix the checksum validations ip_vs_in_icmp_v6() is missing checksum validation for ICMPv6 packets from clients. In fact, as for TCP/UDP we should validate the checksum for ICMP packets only when we mangle the packets on MASQ or on reply for tunnel. Also, Sashiko points out that handle_response_icmp() being common for IPv4 and IPv6 is missing the pseudo-header calculation while validating ICMPv6 messages from real servers which is a problem if checksum is not validated by the hardware. Fix the problems by creating ip_vs_checksum_common_check() helper and use it for TCP/UDP/ICMP both for IPv4 and IPv6. Rely on the nf_checksum() for validating the ICMP messages but use it also for TCP and UDP. Use correct IP offset for IP_VS_DBG_RL_PKT for TCP/UDP/SCTP. IPVS packets (TCP/UDP/SCTP/ICMP) do not need checksum validation on LOCAL_OUT (local clients or local real servers) and on FORWARD (traffic from servers on LAN). Do it only on LOCAL_IN, in case nf_checksum() is not called on PRE_ROUTING. Also, ip_vs_checksum_complete() can be marked static.	N/A	More Details
CVE-2026-79390	Trueview TI8161 6.0.23.4 is vulnerable to information disclosure due to the transmission of MQTT communications in plaintext over TCP port 1883. An unauthenticated attacker with access to the same network segment can intercept MQTT traffic and obtain sensitive device information and operational data, including device identifiers, message metadata, and control-related information.	N/A	More Details
CVE-2022-26961	Italtel NetMatch-S 5.0.0-20200703 allows Multiple Stored XSS under NP_IBCF-NATUP-01/NMSCI-WebGui/backup_restore.jsp and NP_IBCF-MIBER-03/NMSCI-WebGui/storage.jsp via the name parameter. A malicious user leveraging this vulnerability could inject arbitrary JavaScript. The malicious payload will then be triggered every time an authenticated user browses the page containing it.	N/A	More Details
CVE-2026-50894	easyadmin v2.0.2.2 is vulnerable to Unrestricted Upload of File with Dangerous Type in the background management interface which allows authenticated remote attackers to execute arbitrary code and gain server privileges via a crafted file upload.	N/A	More Details
CVE-2026-14297	A buffer overflow in the Bluetooth Continuous Glucose Monitoring Service (CGMS) Record Access Control Point (RACP) write handler allows an authenticated BLE peer to overflow a 20-byte static buffer into adjacent BSS memory. The exploitable impact cannot be predetermined - it is entirely dependent on the linker-assigned BSS layout of the specific firmware build, which may vary.	N/A	More Details
CVE-2026-16876	An authentication bypass vulnerability exists in the WebGUI of Series UNIVERGE IX-R/IX-V. A user could bypass authentication and execute arbitrary CLI commands by tampering with WebGUI messages and sending them to the device via internet.	N/A	More Details
CVE-2026-78043	The Windows Interactive Service in OpenVPN 2.7_alpha1 through 2.7.6 allows local authenticated users to bypass the trusted configuration directory constraint and load arbitrary configuration files via specially crafted paths	N/A	More Details
CVE-2026-	An incorrect buffer size calculation in the Windows Interactive Service in OpenVPN 2.7_alpha1 through 2.7.6 allows local authenticated users to cause memory corruption or disclose sensitive information via crafted	N/A	More Details

78221	NRPT inputs.		
CVE-2026-81738	OpenVPN 2.5.0 through 2.7.6 on Windows using the tap-windows6 driver allows attackers to trigger an out-of-bounds write via crafted DOMAIN-SEARCH entries	N/A	More Details
CVE-2026-81830	The Windows interactive service in OpenVPN 2.4.0 through 2.6.22 allows local authenticated users to bypass the trusted configuration directory constraint via incorrect file path validation	N/A	More Details
CVE-2026-82312	OpenVPN 2.0.0 through 2.6.22 and 2.7_alpha1 through 2.7.6 on Windows allows local authenticated users to cause a denial of service via a NULL DACL on named IPC objects	N/A	More Details
CVE-2026-84226	OpenVPN version 2.5.0 through 2.6.22 and 2.7_alpha1 through 2.7.6 on Windows allows local authenticated users to perform a binary planting attack during network configuration steps	N/A	More Details
CVE-2026-84256	An argument parsing issue in OpenVPN 2.1_rc10 through 2.6.22 and 2.7_alpha1 through 2.7.6 on Windows allows remote authenticated users to execute arbitrary commands via a crafted certificate subject	N/A	More Details
CVE-2026-18796	Any application that uses external QSPI flash for encrypted XIP on nRF5340 and relies on that encryption for confidentiality and/or integrity of the externally stored code. No specific nRF Connect SDK version is the root cause; the weakness is in the on-the-fly decryption scheme.	N/A	More Details
CVE-2026-82750	Improper Validation of Specified Quantity in Input in ZenHive mpp allows an unauthenticated remote client to inflate the fee-payer's gas cost per sponsored payment by a large multiplier and to have the sponsor pay for EIP-7702 account delegations of the client's choosing. When the server sponsors Tempo payments, MPP.Methods.Tempo.FeePayerPolicy.measure/3 in lib/mpp/methods/tempo/fee_payer_policy.ex bounds the gas fields, the fee budget, the validity window and the access list of the client-signed 0x76 envelope, but never reads its aa_authorization_list field. Every signed delegation in that list is charged as intrinsic gas before the payment call runs, so a client attaching delegations from throwaway authority keys makes the sponsor pay for them within the default gas_limit ceiling. At the reporter's default of seven entries the sponsored cost rises from about 46,575 gas to about 1,884,087 gas. Because each entry is applied as a persistent set-code delegation, a client can also upgrade its own accounts to delegated code at the sponsor's expense. This issue affects mpp: from 0.2.0 before 0.16.1.	N/A	More Details
CVE-2026-84186	Vulnerability involving incorrect access control in the Tools::getRemoteAddr() function in PrestaShop, which allows the client’s IP address to be spoofed via the X-Forwarded-For header when the application is running behind a reverse proxy, load balancer or CDN. The application incorrectly processes the IP address string and uses the address controlled by the visitor rather than the one provided by the trusted infrastructure, allowing an unauthenticated remote attacker to cause the application to interpret their connection as originating from an arbitrary IP address. This condition allows IP-based controls, such as the maintenance mode allowlist, to be bypassed, as well as enabling the forgery of security and audit logs and the evasion of third-party mechanisms that rely on the IP address, such as geolocation checks, fraud detection or request throttling.	N/A	More Details
CVE-2026-84732	Retransmissions of ACK packet ID in OpenVPN through 2.6.22 and 2.7.6 allow remote unauthenticated attackers to cause a denial of service via crafted inputs that trigger a timeout integer overflow	N/A	More Details
CVE-2026-86342	Affected versions of MISP contain improper authorization checks in the freetext feed preview functionality. The preview performed correlation lookups against attributes from events without applying the requesting user's ACL, allowing restricted event correlations and associated event information to be exposed to users who could not otherwise access those events. The vulnerable queries were scoped only by attribute values and deletion status rather than MISP's event, organization, sharing-group, attribute, and object-level access controls. The same preview functionality also returned cross-feed correlation information without properly restricting the feed list to feeds visible to the caller. This exposed metadata for feeds that were not marked lookup_visible; one affected response additionally included the configured feed URL even though that value was not required by the feature. The fixes apply the caller's ACL to attribute correlation searches, remove feed URLs from correlation results, restrict cross-feed results according to feed visibility, and correct host-organization ID comparison so the authorization rules are applied consistently. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-84173	In Eclipse Ankaios versions v0.5.1 through v1.0.1, the agent-side Control Interface authorizer incorrectly evaluates multi-segment allow rules whose first path segment is a wildcard. An authenticated workload with access restricted by such a rule can submit a CompleteStateRequest or UpdateStateRequest with an empty field mask. The request may then be incorrectly authorized as matching the scoped rule, allowing the workload to read the complete cluster state or replace state outside its authorized subtree. This may result in unauthorized disclosure or modification of other workloads and cluster configuration. Only a rule consisting solely of * is intended to authorize an empty mask. Mitigation: Until an update containing the fix is installed, avoid multi-segment Control Interface allow-rule filter masks that begin with a wildcard, such as *.workloads.some_workload. Replace them with explicit paths such as	N/A	More Details

	desiredState.workloads.some_workload, where applicable. A filter mask consisting solely of * has different, intentionally unrestricted semantics and should only be used when full-state access is intended.		
CVE-2026-86347	Affected versions of MISP allow any authenticated user to access TemplatesController::uploadFile() because the ACL entry for templates/uploadFile used the wildcard *. This bypasses the intended role restrictions applied to neighboring template-management operations. The upload handler accepts arbitrary content with only minimal checks and writes it into app/tmp/files/. A low-privileged or read-only user can therefore repeatedly upload files and consume server disk space without requiring perm_add or perm_template. The fix changes the ACL requirement from * to perm_add. The commit also rules out stronger impacts: uploaded files receive random names, path traversal/predictable overwrite is not available, the temporary directory is outside the web root, and the files are not directly served over HTTP. Therefore, the issue should not be described as arbitrary file overwrite, stored XSS, or RCE. Version affected: ≤2.5.45	N/A	More Details
CVE-2026-19204	A client may send a WebSocket frame with an unknown opcode and a very large declared payload length, causing Jetty to attempt a large memory allocation and potentially exhaust the JVM heap. This occurs when auto-fragmentation is enabled, as unknown opcodes bypass the normal maximum frame size handling and payload allocation occurs before the opcode is validated.	N/A	More Details
CVE-2026-82325	A use-after-free vulnerability in the OpenVPN ovpn-dco-win driver version 2.5.0 through 2.8.6 allows local authenticated users to cause a system crash via crafted control messages	N/A	More Details
CVE-2026-85201	In Eclipse Ankaios versions 0.1.0 through 1.0.1, the agent does not limit the length declared by a workload in a length-delimited protobuf message received through the Control Interface FIFO. A workload granted Control Interface access can specify an excessive message length, causing an unbounded memory allocation that may abort the Ankaios agent process. This results in loss of orchestration services for workloads managed by the affected agent.	N/A	More Details
CVE-2026-82751	Improper Validation of Specified Quantity in Input in ZenHive mpp allows an unauthenticated remote client to inflate the fee-payer's gas cost per sponsored payment by a large multiplier and to have the sponsor pay for provisioning an access key on the client's own account. When the server sponsors Tempo payments, MPP.Methods.Tempo.FeePayerPolicy.measure/3 in lib/mpp/methods/tempo/fee_payer_policy.ex bounds the gas fields, the fee budget, the validity window and the access list of the client-signed 0x76 envelope, but does not check whether the envelope carries the optional key_authorization field. A client can attach a fully signed key authorization, provisioning a new access key with token spending limits on its own account, alongside the normal payment call. The key and each limit entry are persistent storage writes billed as intrinsic gas to the sponsor, bounded only by the gas_limit ceiling. At the reporter's default of one key with three token limits the sponsored cost rises from about 46,587 gas to about 1,808,700 gas, and the client keeps a valid access key it paid nothing for. This issue affects mpp: from 0.2.0 before 0.16.1.	N/A	More Details
CVE-2026-86283	MISP's UiBeta theme collection view (app/View/Themed/UiBeta/Collections/view.ctp) performed a secondary query of member events by UUID without applying the caller's access control list (ACL). The CollectionsController::view() action correctly resolved collection element UUIDs through Event::fetchSimpleEvents($user, ...), which enforces per-user event ACL. However, the view template independently re-queried the same UUIDs using only an Event.uuid IN (...) condition, omitting the createEventConditions() authorization filter. Because collection element UUIDs are stored without server-side authorization against the referenced event (CollectionElementsController::add() accepts whatever UUID the collection owner posts), an authenticated user with view access to a collection could retrieve full details of events they are not permitted to read. The exposed data included event identifiers, info, dates, timestamps, creator organization, all event tags, and galaxy clusters (the latter attached via a cluster-scoped rather than event-scoped ACL check). This constitutes an authorization bypass at the presentation layer, allowing horizontal privilege escalation across event boundaries within the MISP instance.	N/A	More Details
CVE-2026-75439	An issue in Free5GC v.4.2.2 allows a remote attacker to cause a denial of service via the UPF component	N/A	More Details
CVE-2026-82752	Improper Validation of Specified Quantity in Input vulnerability in ash-project ash allows an attacker to store a value of arbitrary size in an attribute whose length constraint should bound it. Ash measures string length with Elixir's String.length/1, which counts Unicode graphemes, in the max_length and min_length constraints of Ash.Type.String (apply_constraints/2 in lib/ash/type/string.ex), in Ash.Resource.Validation.StringLength, and in the string_length expression function. A grapheme carries an unbounded number of combining marks, so a base character followed by a million combining acute accents is one grapheme and megabytes of data, and satisfies max_length: 2. Where the data layer imposes no independent limit (ETS, Mnesia, or a Postgres text column) the whole value is persisted, so an attacker can write an entire request body into an attribute declared with a small maximum and grow storage without bound. The counting unit also disagrees with the storage layer, which counts codepoints rather than graphemes, so a value accepted by the constraint can still be rejected or truncated by the column. A Postgres varchar(n) column bounds the value itself and is not exposed. This issue affects ash: from 0.10.0 before 3.33.0.	N/A	More Details
	Twig is a template language for PHP. From version 1.0.0 to before version 3.27.0, SecurityPolicy::checkMethodAllowed() unconditionally whitelists all method calls on instances of Twig\Markup.		

CVE-2026-46636	Twig\Markup is not final, so subclasses inherit the bypass. An application that passes an object of a Markup-derived class into a sandboxed template (typically to mark a chunk of HTML as safe) inadvertently exposes every public method of that subclass to template authors, regardless of the configured allowedMethods list. This issue has been patched in version 3.27.0.	N/A	More Details
CVE-2026-52762	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, YesWiki Bazar contains a stored Server-Side Template Injection (SSTI) vulnerability in the semantic template feature that can be escalated to confirmed Remote Code Execution (RCE). An authenticated administrator can place arbitrary Twig expressions into the Semantic template (Twig) field (bn_sem_template), and that content is later executed server-side when public semantic endpoints are requested. This issue has been patched in version 4.6.6.	N/A	More Details
CVE-2026-52777	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, there is an authenticated PHP object injection vulnerability in BazarImportAction via unserialize. This issue has been patched in version 4.6.6.	N/A	More Details
CVE-2026-86193	grav-plugin-api before 1.0.20 fails to validate group-inherited super permissions in user-management guards, allowing non-super user managers to modify super-admin accounts. Attackers with api.access and api.users.write can patch password fields on group-super accounts to gain full administrative control.	N/A	More Details
CVE-2026-86194	Grav Form Plugin before 9.1.22 fails to verify page authorization when resolving forms by name across pages, allowing anonymous visitors to execute form actions defined on login-restricted or unpublished pages. Attackers can POST to any public page with a restricted form's name to trigger save, upload, email, or call actions without authentication.	N/A	More Details
CVE-2026-86195	grav-plugin-api versions before 1.0.20 contain a privilege escalation vulnerability in the InvitationsController where the stripSuperFlags() method only removes nested super flags but fails to strip dot-keyed equivalents like api.super. A non-super user manager with api.access and api.users.write permissions can create an invitation with a dot-keyed super flag in the access payload that bypasses the guard and persists to the new account. Attackers can accept the invitation through the public endpoint without real invitee interaction to create a super-admin account and immediately receive a valid JWT for full site control.	N/A	More Details
CVE-2026-86196	Grav API plugin versions before 1.0.20 build password reset links from the untrusted Host header in the forgot-password endpoint, allowing unauthenticated attackers to redirect reset tokens to attacker-controlled domains. Attackers can send password reset requests for any account with a malicious Host header, intercept the reset token from victim emails, and complete account takeover including super-admin accounts.	N/A	More Details
CVE-2026-86197	Grav before 2.0.20 contains a cross-site scripting vulnerability in the Twig sandbox policy that allowlists addJs and addCss methods on Grav\Common\Assets without proper output escaping. Page editors can inject arbitrary script by registering malicious assets or injecting attributes, which are rendered unescaped into document head tags and executed for all visitors including administrators.	N/A	More Details
CVE-2026-86207	An authentication bypass in N-central < 2026.3 HF 3 leads to authentication bypass in internal only APIs	N/A	More Details
CVE-2026-76161	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-67276	RouterOS does not compare the complete RSA public key when matching an SSH authentication request to an authorized user key, checking the key type and modulus but omitting the exponent. Because signature verification uses the client-supplied key, an attacker knowing an authorized RSA modulus can supply a key with exponent one, forge a valid signature, and open an SSH command channel as the target user without the private key.This issue affects only 7.x branch was fixed in versions: 7.23.4 (Long-term) and 7.24.2 (Stable)	N/A	More Details
CVE-2026-67277	RouterOS accepts a "related" btest connection before the corresponding primary session has completed authentication. An unauthenticated client can use this state to start an IPv4 UDP test. With "random-data=false", the sender transmits an uninitialized tail from a kernel packet buffer. A separate unchecked, inverted packet-size interval causes unsigned integer underflow, anomalously large fragmented output, and can restart the RouterOS kernel. This issue was fixed in versions: 6.49.21 (Long-term), 7.23.4 (Long-term) and 7.24.2 (Stable)	N/A	More Details
CVE-2026-67278	MikroTik RouterOS accepts malformed RSA/PKCS#1 v1.5 signatures during X.509 validation. Because its trust store includes an e=3 root CA, an attacker controlling or redirecting an outbound RouterOS TLS connection can use the root's public certificate - without its private key - to forge a trusted intermediate and issue certificates for arbitrary hostnames, enabling TLS server impersonation. This issue affects only 7.x branch was fixed in versions: 7.23.4 (Long-term) and 7.24.2 (Stable)	N/A	More Details
CVE-2026-	RouterOS SSH enters the connection protocol after a client-requested rekey even though user authentication was never attempted, allowing an unauthenticated client to open a session channel and send an exec request. On affected builds the server dispatches the command, enabling unauthenticated creation,	N/A	More

67279	overwrite, and reconstruction of files in the RouterOS managed file namespace, including support files containing configuration and diagnostic data.This issue was fixed in versions: 6.49.21 (Long-term), 7.23.4 (Long-term) and 7.24.2 (Stable)		Details
CVE-2026-67281	RouterOS WebFig contains an unauthenticated file-read vulnerability in the /jsproxy path where a newly allocated session retains a stale uninitialized principal pointer used for file authorization. An unauthenticated attacker can prepare the allocator so that the file-serving path dereferences this pointer with sufficient rights, then supply parent-directory components in an encrypted URI to escape the WebFig file namespace and disclose root-owned files, including configuration stores containing credentials.This issue affects only 7.x branch was fixed in versions: 7.23.4 (Long-term) and 7.24.2 (Stable)	N/A	More Details
CVE-2026-86060	RouterOS contains an argument-handling flaw in the SSH login path involving usernames that begin with a prohibited character, allowing for the trusted RouterOS policy mask to be changed, leading to privilege escalation. Exploitation requires an unauthenticated SSH session to reach the RouterOS login helper.This issue was fixed in versions: 6.49.21 (Long-term), 7.23.4 (Long-term) and 7.24.2 (Stable)	N/A	More Details
CVE-2026-86206	A vulnerability in the N-central internal API access control filter allows unauthorised access to internal APIs. This is fixed in N-central 2026.3 HF3 and 2026.4	N/A	More Details
CVE-2026-76160	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-57164	PJSIP is a free and open source multimedia communication library written in C. Prior to commit 8d5956a, a heap buffer overflow exists in the PJLIB-UTIL HTTP client (http_client.c) when buffering an HTTP response body. This affects applications that use the PJLIB-UTIL HTTP client to receive a whole response body at once (a completion callback with no incremental on_data_read callback). When growing the response buffer, an incorrect size calculation based on the server-supplied Content-Length can leave the buffer too small, causing response data to be written past the end of the allocation. A malicious or man-in-the-middle HTTP server can trigger this with a crafted response; impact may range from unexpected application termination to memory corruption. Applications that consume the response incrementally (via on_data_read), or that only connect to trusted servers, are not affected. This issue has been patched via commit 8d5956a.	N/A	More Details
CVE-2026-57162	PJSIP is a free and open source multimedia communication library written in C. Prior to commit a1b707c, a stack buffer overflow exists in the SRTP/SDES media transport when processing a=crypto attributes during SDP offer/answer (sdes_encode_sdp() in transport_srtp_sdes.c). This affects applications with SRTP enabled (use_srtp optional or mandatory, using SDES keying). During media negotiation, the crypto attributes from the remote SDP are collected into a fixed-size array without bounding their number; a remote peer that includes an excessive number of a=crypto attributes in a single media description can write past the end of that array on the stack. This is reachable from an incoming SIP INVITE during offer/answer, before application-level authentication. Impact may range from unexpected application termination to control flow hijack/memory corruption. Applications that do not enable SRTP are not affected. This issue has been patched via commit a1b707c.	N/A	More Details
CVE-2026-80812	In the Linux kernel, the following vulnerability has been resolved: ALSA: dummy: Check card index validity at probe snd_dummy_probe() blindly trusts that the given devptr->id value is within the proper card index range. It's OK for the devices the driver itself creates at the module probe time, but if the device is bound manually via sysfs interface, this could be -1 as "none", and this leads to OOB access for index[] and other parameters. Add a sanity check for the card index and warn/correct it if it's a value out of the range.	N/A	More Details
CVE-2026-57161	PJSIP is a free and open source multimedia communication library written in C. Prior to commit acc03b5, a stack buffer overflow exists in PJSUA when processing Service-Route headers in a registration response (update_service_route() in pjsua_acc.c). This affects applications that register using the PJSUA/PJSUA2 account API (the default registration path). The Service-Route URIs from a 2xx response to REGISTER are stored into a fixed-size array without bounding the number of headers; a registrar that returns an excessive number of Service-Route headers can write past the end of the array on the stack. The values written are internal pointers rather than arbitrary data, so the most likely impact is unexpected application termination (denial of service), though memory corruption cannot be excluded. The malicious response may come from a compromised or malicious registrar, or — over unprotected transports — a spoofed response. This issue has been patched via commit acc03b5.	N/A	More Details
CVE-2026-80835	In the Linux kernel, the following vulnerability has been resolved: crypto: qcom-rng - Remove crypto_rng interface qcom-rng.c exposes the same hardware through two completely separate interfaces, crypto_rng and hwrng. However, the implementation of this is buggy because it permits generation operations from these interfaces to run concurrently with each other, accessing the same registers. That is, qcom_rng_generate() synchronizes with itself but not with qcom_hwrng_read(). This results in potential repetition of output from the RNG, output of non-random values, etc. Fortunately, there's actually no point in hardware RNG drivers implementing the crypto_rng interface. It's not actually used by anything besides the "rng" algorithm type of AF_ALG, which in turn is not actually used in practice. Other crypto_rng hardware drivers are likewise being phased out, leaving just the hwrng support. Thus, remove it to simplify the code	N/A	More Details

	and avoid conflict (and confusion) with the hwrng interface which is the one that actually matters.		
CVE-2026-80836	In the Linux kernel, the following vulnerability has been resolved: crypto: virtio - bound the akcipher result length virtio_crypto_dataq_akcipher_callback() sets the result length from the device-reported response length without bounding it to the destination buffer, which was allocated for the original request length. sg_copy_from_buffer() then reads that many bytes from the destination buffer; a backend reporting a larger length over-reads adjacent kernel heap into the caller's scatterlist (an out-of-bounds read). Clamp the reported length to the originally requested destination length. A conforming device reports no more than that, so valid results are unaffected.	N/A	More Details
CVE-2026-80837	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: don't queue packet path object notifications All file:line references below are against v7.2-rc4 (ac5b0e5651b1). The trace was captured on 7.2.0-rc6-kasan72rc6 (075b74841bd0), where the same lines apply. nft_obj_notify() is exported and reached from the packet path. Its only in-tree caller is nft_quota_obj_eval() (net/netfilter/nft_quota.c:68), which notifies with GFP_ATOMIC while evaluating a rule for a transiting packet, holding no mutex. Since commit 67cc570edaa0 ("netfilter: nf_tables: coalesce multiple notifications into one skbuff") that notification is no longer sent immediately. __nft_obj_notify() queues it onto nft_net->notify_list via nft_notify_enqueue() (net/netfilter/nf_tables_api.c:1211), which is a bare list_add_tail(). notify_list has no lock of its own (include/net/netfilter/nf_tables.h:1951), it is serialised by commit_mutex: the six other enqueue sites all run inside a netlink transaction, and the drain in nft_commit_notify() (net/netfilter/nf_tables_api.c:10746) does list_del() + kfree_skb() from nf_tables_commit() with commit_mutex held. Sending packets through a chain that references a depleted quota object therefore races an unlocked list_add_tail() against list_del() + kfree_skb() on another CPU. The WRITE_ONCE(prev->next, new) in __list_add() then stores through an sk_buff that has already been freed: BUG: KASAN: slab-use-after-free in __nft_obj_notify+0x2c5/0x2d0 Write of size 8 at addr ff110001047183c0 by task poc/76 CPU: 0 UID: 1000 PID: 76 Comm: poc Tainted: G W 7.2.0-rc6-kasan72rc6 #4 Call Trace: <IRQ> __nft_obj_notify (include/linux/list.h:164 include/linux/list.h:191 net/netfilter/nf_tables_api.c:1211 net/netfilter/nf_tables_api.c:8743) nft_quota_obj_eval (net/netfilter/nft_quota.c:68) nft_do_chain_inet nf_hook_slow __ip_local_out ip_push_pending_frames udp_send_skb udp_sendmsg __x64_sys_sendto Allocated by task 77: __alloc_skb (net/core/skbuff.c:704) __nft_obj_notify (include/net/netlink.h:1055 net/netfilter/nf_tables_api.c:8731) nft_quota_obj_eval (net/netfilter/nft_quota.c:68) nft_do_chain Freed by task 79: nf_tables_commit (include/linux/skbuff.h:1332 net/netfilter/nf_tables_api.c:10759 net/netfilter/nf_tables_api.c:11185) nfnetlink_rcv_batch (net/netfilter/nfnetlink.c:574) netlink_unicast netlink_sendmsg The buggy address belongs to the cache skbuff_head_cache of size 232 Queueing from the packet path is wrong even leaving the race aside: notify_list is only drained by nft_commit_notify() from nf_tables_commit() (:11185), so a notification enqueued outside a transaction is not sent until some later netlink batch commits, if one ever does. The gfp argument that nft_obj_notify() still takes is a leftover of the pre-67cc570edaa0 behaviour, where this path called nfnetlink_send() directly. Restore that: split the message construction out into nft_obj_notify_alloc() and let each caller decide what to do with the skb. nft_obj_notify(), the exported one reached from the packet path, sends it straight away; nf_tables_obj_notify(), which runs under commit_mutex, keeps queueing it, so transaction notifications are still coalesced.	N/A	More Details
CVE-2026-80838	In the Linux kernel, the following vulnerability has been resolved: vxlan: keep the last remote linked during FDB flush A non-nexthop FDB entry is expected to have at least one remote while it remains reachable through the FDB hash table. A filtered bulk flush violates this invariant when every remote matches: It unlinks the last remote in vxlan_fdb_dst_destroy() and only afterwards tells vxlan_flush() to destroy the parent FDB entry. An RCU reader can find the parent during this interval. first_remote_rcu() then applies list_entry_rcu() to the empty list head, producing an invalid remote pointer that the receive learning path can read from and write to. When a matching remote is the sole remaining remote, leave it linked and ask the caller to destroy the entire FDB entry. vxlan_fdb_destroy() keeps the remote attached while sending the deletion notification and removing the parent from the lookup structures.	N/A	More Details
CVE-2026-80839	In the Linux kernel, the following vulnerability has been resolved: batman-adv: reject unrepresentable multicast TVLV offsets The network and transport header fields in struct sk_buff are 16-bit offsets from skb->head, and U16_MAX is reserved as the unset transport header value. batadv_tvlv_call_handler() sets both fields from a received multicast TVLV without checking whether the TVLV end is representable. If the end offset exceeds the field's range, skb_set_transport_header() truncates it so that the transport header precedes the network header. The negative difference is then returned by skb_network_header_len() as a large u32. batadv_mcast_forw_packet() consequently accepts an oversized multicast tracker and accesses memory beyond the skb data. Add skb_set_transport_header_careful(), an offset-aware counterpart to skb_reset_transport_header_careful(), which validates the final head-relative offset before assigning it. Use the new helper in batadv_tvlv_call_handler() and reject unrepresentable TVLVs before setting the network header.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: ipv6: seg6: clear IPv4 control block on IPIP decapsulation End.DX4 and End.DT4 decapsulate an IPv4 packet through decap_and_validate() and send it directly to IPv4 routing. The inner packet therefore bypasses ip_rcv_core(), which normally clears IPCB before IPv4 interprets skb->cb. The skb instead retains IP6CB data from the outer packet. IP6CB and IPCB use the same skb->cb storage, so IP6CB(skb)->lastopt overlaps IPCB(skb)->opt.optlen and srr, while IP6CB(skb)->nhoff overlaps rr and ts. The sender can make the stale optlen byte nonzero with a valid outer extension-header chain. The reproducers put an eight-byte Destination Options header immediately after the 40-byte		

CVE-2026-80840	IPv6 header and before the Segment Routing Header. ipv6_destopt_rcv() records the sender-controlled Destination Options offset in both lastopt and nhoff, setting them to 40. On the reproduced little-endian x86-64 kernel, IPv4 therefore sees optlen = 40 and rr = 40. Both tcp_v4_save_options() and __ip_options_echo() skip option copying when optlen is zero. Here optlen is 40, so the TCP SYN path allocates room for 40 bytes of option data and calls __ip_options_echo(). The stale rr value makes that function read inner packet byte 41 as the Record Route option length. The reproducers set that sender-controlled byte to 255, so __ip_options_echo() copies 255 bytes into the 40-byte option-data area. Separate End.DX4 and End.DT4 reproducers on the unpatched v7.2-rc5 kernel both produced: BUG: KASAN: slab-out-of-bounds in __ip_options_echo() Write of size 255 The relevant End.DX4 call path is: __ip_options_echo tcp_v4_route_req tcp_conn_request tcp_v4_conn_request tcp_rcv_state_process tcp_v4_do_rcv tcp_v4_rcv ip_protocol_deliver_rcu ip_local_deliver_finish ip_local_deliver input_action_end_dx4_finish input_action_end_dx4 The relevant End.DT4 call path is: __ip_options_echo tcp_v4_route_req tcp_conn_request tcp_v4_conn_request tcp_rcv_state_process tcp_v4_do_rcv tcp_v4_rcv ip_protocol_deliver_rcu ip_local_deliver_finish ip_local_deliver input_action_end_dt4 tcp_v4_save_options() is inlined into the tcp_v4_route_req() path, so it does not appear as a separate frame. When decap_and_validate() handles IPPROTO_IPIP, save the ingress interface from IP6CB, clear IPCB, and restore the saved value. Doing this in the common decapsulation path covers End.DX4, End.DT4, and End.DT46's IPv4 arm. Use IP6CB(skb)->iif rather than skb->skb_iif. These actions run after l3mdev processing, which can replace skb_iif with the L3 master; IP6CB iif still records the receiving interface set at IPv6 ingress.	N/A	More Details
CVE-2026-80841	In the Linux kernel, the following vulnerability has been resolved: net/packet: defer vmalloc TX_RING free until skbs finish AF_PACKET TX_RING skbs keep a raw pointer to their ring frame. The skb page references preserve page-backed ring blocks after pg_vec is freed, but they do not preserve a vmalloc mapping. tpacket_destruct_skb() currently drops the pending reference before writing the timestamp and TP_STATUS_AVAILABLE to the frame. Move the decrement after those stores. The smp_wmb() in __packet_set_status() orders the frame stores before the decrement. Also recheck pending TX frames under pg_vec_lock before non-closing ring replacement, so a racing send cannot add a pending skb between the initial check and the ring swap. Ring allocation can produce a mixture of page-backed and vmalloc-backed blocks. Allocate deferred-work storage during TX ring setup when the first vmalloc-backed block is encountered, and keep its pointer in the pg_vec allocation header. If allocation fails, return -ENOMEM from ring setup. On socket close, a non-NULL pointer identifies a vmalloc-backed vector without a scan. If TX skbs remain, defer the whole vector to system_long_wq. After pg_vec is detached, a late destructor can skip the pending decrement. Use socket write-memory accounting as the deferred lifetime gate instead: an skb remains charged through its final sock_wfree(), after all ring-frame accesses. The delayed work retains a socket reference and reschedules itself until no TX skbs remain. Move pending_refcnt release to packet_sock_destruct() so late skb destructors and deferred cleanup can safely use it after packet_release(). Page-backed teardown remains synchronous, and no lock is added to the TX completion hot path.	N/A	More Details
CVE-2026-80842	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: fix use-after-free of a master VLAN's multicast context br_multicast_toggle_one_vlan() clears BR_VLFLAG_MCAST_ENABLED under br->multicast_lock before stopping a VLAN's multicast context. That is the teardown handshake: lockless readers gate on the flag through br_multicast_ctx_should_use() -> br_multicast_ctx_vlan_disabled(), so once it is cleared under the lock no reader can arm the context again. For a master VLAN the handshake never runs. __vlan_del() clears BRIDGE_VLAN_INFO_BRENTRY before calling br_vlan_put_master(), so br_multicast_toggle_one_vlan(masterv, false) returns early on !br_vlan_is_brentry(vlan): the flag stays set and br->multicast_lock is never taken. br_vlan_put_master() then drains the context in br_multicast_ctx_deinit() and frees the VLAN through call_rcu(), while a reader still inside rcu_read_lock() sees the context as enabled and re-arms it. The port and port-VLAN branch of the function has no br_vlan_is_brentry() test and flips the flag under br->multicast_lock, so it is not affected. The reader is the bridge transmit path. For a master VLAN br_multicast_rcv() selects brmctx = &vlan->br_mcast_ctx with pmctx = NULL, so IGMP sent to the bridge device re-arms the context's timers after br_multicast_ctx_deinit() has already stopped them. BUG: KASAN: slab-use-after-free in detach_if_pending+0x412/0x4a0 Write of size 8 at addr ffff88810ac39918 by task brmc/601 __mod_timer+0x51a/0xc50 br_multicast_host_join+0x25b/0x390 __br_multicast_add_group+0x468/0x530 br_ip4_multicast_add_group+0x1a0/0x260 br_multicast_rcv+0x2cda/0x61e0 br_dev_xmit+0x6c4/0x1540 Allocated by task 610: br_vlan_add+0x111/0xb40 br_vlan_info+0x370/0x3e0 Freed by task 0: kfree+0x1a7/0x4f0 rcu_core+0x7dc/0x10a0 Only test br_vlan_is_brentry() when enabling, like the br_multicast_ctx_vlan_global_disabled() test next to it. Disabling then always clears BR_VLFLAG_MCAST_ENABLED under br->multicast_lock before br_multicast_ctx_deinit() drains the context.	N/A	More Details
CVE-2026-80843	In the Linux kernel, the following vulnerability has been resolved: xfrm: fix xfrm_state_construct() auth-trunc leak attach_auth_trunc() can allocate x->aalg while leaving x->props.aalgo at zero when the selected auth algorithm has no sadb_alg_id. One real case is cmac(aes). xfrm_state_construct() then treats !x->props.aalgo as "no auth algorithm attached yet" and calls attach_auth(). That overwrites x->aalg and loses the first allocation. Any later failure or teardown only frees the replacement pointer. Check whether x->aalg is already attached instead of inferring that state from x->props.aalgo.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: xfrm: ah6: validate routing header segments_left AH6 rearranges routing-header addresses before computing or verifying the ICV. ipv6_rearrange_rthdr() assumes that segments_left is not larger than the number of addresses described by		

CVE-2026-80844	the routing header's hdrlen field. That assumption does not hold for raw IPv6 HDRINCL packets. A packet with hdrlen equal to 2 describes one address, but can carry an arbitrary segments_left value. With segments_left equal to 255, the function moves its address pointer 4,064 bytes backwards and passes a 4,064-byte length to memmove(), resulting in an out-of-bounds access. Validate the invariant locally before modifying the routing header or performing any address-pointer arithmetic, and propagate malformed-header errors to the existing AH6 input and output error paths.	N/A	More Details
CVE-2026-80845	In the Linux kernel, the following vulnerability has been resolved: xfrm: avoid lock inversion in nat keepalive work nat_keepalive_work() walks the state table while xfrm_state_walk() holds net->xfrm.xfrm_state_lock. Its callback then acquires x->lock, which conflicts with the delete path taking the same locks in reverse order via xfrm_state_delete() and __xfrm_state_delete(). This creates an AB-BA deadlock that is reported by lockdep when a NAT keepalive worker races with SA deletion. Fix this by splitting the keepalive walk into two phases. First, collect the candidate states while the walk holds xfrm_state_lock and take a reference on each state. Then, after the walk completes, process each collected state and acquire x->lock without nesting it under xfrm_state_lock.	N/A	More Details
CVE-2026-80846	In the Linux kernel, the following vulnerability has been resolved: xfrm: drop ESP-in-TCP packets with no ingress device ESP-in-TCP receives records through the TCP strparser. handle_esp() restores skb->dev from the saved skb_iif before passing the packet into the XFRM input path. Queued TCP data can be processed after the original ingress device has been removed, for example during veth or net namespace teardown. In that case dev_get_by_index_rcu() returns NULL. The XFRM IPv4 and IPv6 input paths both expect skb->dev to be valid while building the route lookup, so queued ESP-in-TCP data can dereference a NULL device. Drop the packet if the saved ingress device can no longer be resolved. Such a packet can no longer be routed through the normal XFRM receive path, and this preserves the existing behaviour for packets whose ingress device still exists.	N/A	More Details
CVE-2026-80847	In the Linux kernel, the following vulnerability has been resolved: tcp: clamp route advmss to TCP_MIN_MSS tcp_select_initial_window() assumes that callers never pass an MSS smaller than 1, but route-derived advmss values can violate that assumption. A too-small explicit RTAX_ADVMSS is one way to get there, but it is not the only one. The same divide-by-zero can also be reached through the "default advmss" path when RTAX_ADVMSS is left at 0 and the effective advmss is later driven down by route MTU and min_adv_mss. Introduce a tcp_dst_advmss() helper that clamps route advmss to TCP_MIN_MSS before TCP consumes it, and use it in the TCP paths that derive advmss from dst metrics. This keeps the effective MSS from dropping to zero before tcp_select_initial_window() rounds the receive window.	N/A	More Details
CVE-2026-80848	In the Linux kernel, the following vulnerability has been resolved: xfrm: espintcp: fix UAF during close ZDI reported and analyzed a race condition during close for espintcp sockets: espintcp_close() frees emsg->skb via kfree_skb() without holding any socket lock. Concurrently, the xfrm_trans_reinject work queue invokes esp_output_tcp_finish() -> espintcp_push_skb() -> espintcp_push_msgs() -> skb_send_sock_locked(), which reads the same skb as a data source. Fix this by adding a synchronize_rcu() call after resetting sk_prot, since esp_output_tcp_finish() runs under RCU and won't use a socket with sk_prot == &tcp_prot. Simply taking the socket lock in espintcp_close() could lead to leaks, if esp_output_tcp_finish() re-adds an skb in the slot we just freed. After this, the existing barrier() is no longer needed.	N/A	More Details
CVE-2026-80849	In the Linux kernel, the following vulnerability has been resolved: net/tcp-ao: fix use-after-free of current_key on reconnect to another peer tcp_inbound_ao_hash() is called before bh_lock_sock_nested() is taken, with only rcu_read_lock() held. On the fast path for established sockets, if the rnext_keyid sent by the peer differs from current_key->sndid, the key the peer asked for is looked up and stored in current_key. The lookup is inside the RCU read side, but current_key outlives it. When the socket is disconnected and connect() is called again for another peer, tcp_ao_connect_init() unlinks every key that does not match the new peer and frees it with call_rcu(). If current_key points at such a key, it is cleared to NULL. The fast path reads sk_state only once on entry, so a softirq that got into it while the socket was still established can update current_key after that loop has already run. The update is inside the RCU read side, so it comes before the call_rcu() callback, and once the callback frees the key, current_key is left pointing at freed memory. The next transmission picks that pointer up in tcp_get_current_key(). tcp_ao_transmit_skb() then reads the traffic key from the freed object, which is the use-after-free. Wait for one grace period before unlinking, and only if a key is going to be removed. By the time tcp_connect() runs the socket is already in TCP_SYN_SENT, and TCP_AO_ESTABLISHED does not contain TCPF_SYN_SENT, so a softirq entering after the wait cannot reach the fast path, and the ones already in it have finished. The existing NULL handling in the loop is then enough.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: tcp: fix AO info use-after-free in tcp_ao_connect_init() tcp_v4_connect() adds a SYN-SENT socket to the ehash before calling tcp_connect(). If TCP-AO is configured, tcp_connect() first verifies that a key matches the peer and the bound device's current L3 master. tcp_ao_connect_init() later resolves the L3 master again and removes keys which do not match it. The socket lock does not stabilize the bound device's VRF membership. Detaching the device from its VRF between the initial validation and the L3-master calculation in tcp_ao_connect_init() can therefore make the validation succeed while initialization observes the default L3 domain and removes the only key. The subsequent AO lookup then fails, so the no-key path clears tp->ao_info and frees it directly. The receive path can find the socket in the ehash and load tp->ao_info under RCU before acquiring the socket lock. A reader which loaded the old pointer can thus continue into tcp_inbound_ao_hash() after the direct free. The issue was found during a static audit of TCP-AO object lifetime. An unprivileged reproducer in self-created user and		

CVE-2026-80850	network namespaces raced connect() with detaching a veth from its VRF while sending TCP-AO segments. It triggered the same KASAN report on two fresh boots: BUG: KASAN: slab-use-after-free in tcp_inbound_ao_hash+0x585/0x19f0 Write of size 8 at addr ffff88800bf88128 by task tcp_ao_vrf_race/232 Call Trace: tcp_inbound_ao_hash+0x585/0x19f0 tcp_inbound_hash+0x677/0xa80 tcp_v4_rcv+0x1c3e/0x3ab0 Allocated by task 235: tcp_ao_alloc_info+0x43/0xf0 tcp_ao_add_cmd+0xdf7/0x13b0 do_tcp_setsockopt+0x168c/0x2640 Freed by task 235: kfree+0x1b8/0x550 tcp_connect+0x252/0x4f00 tcp_v4_connect+0x1114/0x1720 The bad address is 40 bytes inside the freed 128-byte object, matching the tcp_ao_info counters.key_not_found field. The two runs used 1000 attempts each, reached the no-key path 366 and 411 times, and produced one and two KASAN reports respectively. With this change, the same reproducer reached the no-key path 366 times in 1000 attempts without a KASAN report or oops. Use tcp_ao_destroy_sock() for the no-key path. It unpublishes the AO info, updates the socket memory and static-key accounting, and defers the free until after an RCU grace period. Also drop the WARN_ON_ONCE() and its stale comment. The VRF detach race makes the no-key state reachable during normal operation, so it is a handled condition rather than an impossible assertion. On panic_on_warn kernels the WARN would turn this handled race into a kernel panic.	N/A	More Details
CVE-2026-80851	In the Linux kernel, the following vulnerability has been resolved: gtp: serialize PDP context updates PDP contexts can be deleted through GTP_CMD_DELPDP or while the GTP network device is being unregistered. The latter is serialized by RTNL, but the generic-netlink delete path only holds RCU. Running both paths concurrently can therefore make both paths delete the same PDP context. The issue was found through static analysis and reproduced on a KASAN-enabled kernel by a simple two-thread program racing GTP_CMD_DELPDP against RTM_DELLINK: Oops: general protection fault, probably for non-canonical address KASAN: maybe wild-memory-access in range [0xdead000000000120-0xdead000000000127] RIP: gtp_genl_del_pdp+0x1c1/0x420 [gtp] RBP: dead000000000122 The second deletion dereferenced the poisoned hlist pprev pointer. Serialize gtp_pdp_add(), gtp_genl_del_pdp(), and gtp_dellink() with a shared mutex. Keep the mutex held until the final use of a PDP context in the NEWPDP path, and keep the RCU read-side section around the complete PDP context use in the DELPDP path.	N/A	More Details
CVE-2026-80852	In the Linux kernel, the following vulnerability has been resolved: tls: device: fix out-of-bounds write in tls_append_frag() Found with syzkaller and a local syzbot instance running on top of a netdevsim TLS offload emulation; tls_device.c is otherwise only reachable on a machine with a NIC that implements the offload. tls_push_data() only checks whether the open record still has room for another frag at the bottom of its loop, and the MSG_MORE early break skips that check. The record survives to the next syscall with the frag count it already had, and tls_append_frag() does not check either, so with TLS_TX_ZEROCOPY_RO every splice(SPLICE_F_MORE) of a byte or two adds a non-coalescing pipe page and num_frags walks off the end of tls_record_info.frags[MAX_SKB_FRAGS]. Once the record is pushed, tls_push_record() runs the same index over sg_tx_data[MAX_SKB_FRAGS] and the sg_set_page() writes land on the destruct_work that follows it, which the workqueue then calls. The byte limit is fine because copy drops to 0 and the loop falls through to the same check; the frag count has no such feedback. Push the record rather than keep a full one open, which is what a plain TCP socket does - tcp_sendmsg_locked() uses tcp_mark_push() and new_segment in both the copy and the MSG_SPLICE_PAGES paths, and tls_sw already sets full_record when the sk_msg ring fills up, MSG_MORE or not. BUG: KASAN: slab-out-of-bounds in tls_append_frag (net/tls/tls_device.c:269) Write of size 8 at addr ffff8881104d1530 by task tls_oob/450 CPU: 2 UID: 0 PID: 450 Comm: tls_oob Not tainted 7.2.0-rc7+ #329 PREEMPT Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:94 lib/dump_stack.c:120) print_report (mm/kasan/report.c:378 mm/kasan/report.c:482) kasan_report (mm/kasan/report.c:595) tls_append_frag (net/tls/tls_device.c:269) tls_push_data (net/tls/tls_device.c:518) tls_device_sendmsg (net/tls/tls_device.c:583) inet_sendmsg (net/ipv4/af_inet.c:865) sock_sendmsg (net/socket.c:775 net/socket.c:790 net/socket.c:813) splice_to_socket (fs/splice.c:884) do_splice (fs/splice.c:936 fs/splice.c:1349) __do_splice (fs/splice.c:1431) __x64_sys_splice (fs/splice.c:1634 fs/splice.c:1616) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) </TASK> and, once the record is pushed: UBSAN: array-index-out-of-bounds in net/tls/tls_device.c:300:24 index 18 is out of range for type 'skb_frag_t [17]' UBSAN: array-index-out-of-bounds in net/tls/tls_device.c:301:41 index 18 is out of range for type 'scatterlist [17]' UBSAN: array-index-out-of-bounds in net/tls/tls_device.c:302:39 index 18 is out of range for type 'scatterlist [17]' UBSAN: array-index-out-of-bounds in net/tls/tls_device.c:307:38 index 26 is out of range for type 'scatterlist [17]' kernel tried to execute NX-protected page - exploit attempt? (uid: 0) BUG: unable to handle page fault for address: ffffea000411a680 #PF: supervisor instruction fetch in kernel mode #PF: error_code(0x0011) - permissions violation Oops: Oops: 0011 [#1] SMP KASAN PTI Workqueue: ktls_device_destruct 0xffffea000411a680 RIP: 0010:0xffffea000411a680 Call Trace: <TASK> worker_thread (kernel/workqueue.c:3405 kernel/workqueue.c:3486) kthread (kernel/kthread.c:436) ret_from_fork (arch/x86/kernel/process.c:158) ret_from_fork_asm (arch/x86/entry/entry_64.S:245) </TASK>	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Allocate full pages for {DE,EN}CRYPT ops on SNP-enabled hosts When {de,en}crypting memory of an SEV or SEV-ES guest on an SNP-enabled host via a temporary buffer, allocate a full 4KiB page for the buffer to ensure the page containing the buffer is wholly owned by KVM, i.e. won't be concurrently allocated and accessed by other kernel code while KVM is using the buffer to {de,en}crypt memory. On SNP-enabled platforms, when sending SEV/SEV-ES commands that trigger firmware writes to memory, the to-be-written page(s) must be (temporarily) assigned to Firmware (as required by the SNP architecture, to guard against using such commands as gadgets to attack SNP guests). See snp_map_cmd_buf_desc() and friends. Unfortunately,		

CVE-2026-80853	transferring ownership of a page to Firmware makes the page inaccessible to software, and thus writes generate RMP #PF violations. If KVM uses a sub-page allocation for its temporary buffer, some other actor in the kernel can allocate and use the other portions of the page, and thus trigger unexpected (and seemingly spurious) RMP #PF violations due to software attempting to access a Firmware-owned page. BUG: unable to handle page fault for address: ffff906ae30f0300 #PF: supervisor write access in kernel mode #PF: error_code(0x80000003) - RMP violation PGD 6b1b80d067 P4D 6b1b80d067 PUD 100231e2063 PMD 10055a88063 PTE 80000100630f0163 SEV-SNP: PFN 0x100630f0 unassigned, dumping non-zero entries in 2M PFN region: [0x10063000 - 0x10063200] Oops: Oops: 0003 [#1] SMP CPU: 70 UID: 0 PID: 10658 Comm: svw_WaiterThrea Tainted: G U W O 7.1.0-smp--c22293789940-seanjc-next #1 PREEMPTLAZY Tainted: [U]=USER, [W]=WARN, [O]=OOT_MODULE Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 34.86.0-102 01/25/2026 RIP: 0010:memset+0xf/0x20 Call Trace: <TASK> __kvmalloc_node_noprof+0x2a4/0x710 do_getxattr+0x4e/0x130 path_getxattrat+0x125/0x1b0 do_syscall_64+0x10a/0x480 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7f3a22cb6daa </TASK> Modules linked in: kvm_amd kvm irqbypass vfat fat ccp k10temp sha3 libsha3 i2c_piix4 gq(O) cdc_acm xhci_pci xhci_hcd gsmi: Log Shutdown Reason 0x03 CR2: ffff906ae30f0300 ---[end trace 0000000000000000]--- RIP: 0010:memset+0xf/0x20 Kernel panic - not syncing: Fatal exception Kernel Offset: 0x39e00000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff) gsmi: Log Shutdown Reason 0x02	N/A	More Details
CVE-2026-80834	In the Linux kernel, the following vulnerability has been resolved: crypto: sun8i-ce - Remove crypto_rng interface Since the crypto_rng interface for hardware PRNGs is unused and is redundant with hwrng and the actual Linux RNG, it's being phased out. Most drivers for it were already removed. Go ahead and remove the sun8i-ce support which is one of the only remaining ones. Note that the sun8i-ce support for hwrng remains in place. That is the interface that actually matters. As usual for crypto_rng, this driver was also buggy: its ->generate() function had a use-after-free vulnerability due to using wait_for_completion_interruptible_timeout() without handling shutting down the DMA operation if a signal is sent. There's no point in fixing this separately only to remove the code anyway, so this commit is marked with Fixes and Cc stable.	N/A	More Details
CVE-2026-80833	In the Linux kernel, the following vulnerability has been resolved: crypto: sun8i-ss - Remove crypto_rng interface Since the crypto_rng interface for hardware PRNGs is unused and is redundant with hwrng and the actual Linux RNG, it's being phased out. Most drivers for it were already removed. Go ahead and remove the sun8i-ss support which is one of the only remaining ones. As usual for crypto_rng, this driver was also buggy: its ->generate() function had a use-after-free vulnerability due to using wait_for_completion_interruptible_timeout() without handling shutting down the DMA operation if a signal is sent. Also, it had a buffer overread bug in the line 'memcpy(ctx->seed, d + dlen, ctx->slen);'. There's no point in fixing these bugs separately only to remove the code anyway, so this commit is marked with Fixes and Cc stable.	N/A	More Details
CVE-2026-80832	In the Linux kernel, the following vulnerability has been resolved: crypto: qce - fix CCM AAD buffer underallocation The AAD buffer allocated in qce_aead_ccm_prepare_buf_assoclen() can be smaller than the length later programmed into the DMA scatterlist. The allocation size is currently calculated as: ALIGN(assoclen, 16) + MAX_CCM_ADATA_HEADER_LEN while the DMA length is set to: ALIGN(assoclen + adata_header_len, 16) Since ALIGN() does not distribute over addition, the allocation can be smaller than the DMA length. For example, when assoclen = 32 and adata_header_len = 2: allocation = ALIGN(32, 16) + 6 = 38 DMA length = ALIGN(32 + 2, 16) = 48 As a result, the QCE hardware can read beyond the allocated buffer while computing the CBC-MAC over the associated data. The extra bytes are folded into the authentication tag, resulting in an incorrect tag and causing CCM self-test failures such as: alg: aead: ccm-aes-qce encryption test failed (wrong result) on test vector 8 Fix the allocation by adding the maximum possible AAD header length before alignment: ALIGN(assoclen + MAX_CCM_ADATA_HEADER_LEN, 16) This guarantees that the allocated buffer is large enough for the fully padded AAD data for all supported header sizes.	N/A	More Details
CVE-2026-80821	In the Linux kernel, the following vulnerability has been resolved: nvmet: pci-epf: put CQ ref on create_cq mapping failure nvmet_pci_epf_create_cq() calls nvmet_cq_create(), which takes a reference on the controller and installs the completion queue. If the subsequent PCI address-space mapping fails or returns a too-small partial mapping, the function jumps to err_internal / err_unmap_queue without calling nvmet_cq_put(). The matching put in nvmet_pci_epf_delete_cq() is gated on NVMET_PCI_EPF_Q_LIVE, which is only set after the mapping succeeds, so teardown never releases these references. A remote PCI host that drives Create IO CQ commands with a failing PRP1/pci_addr therefore leaks the CQ and a controller reference on each attempt. Drop the CQ reference on the mapping-failure paths. The err_internal and err_unmap_queue labels are only reachable after nvmet_cq_create() has succeeded, so this pairs the create/put correctly.	N/A	More Details
CVE-2026-80813	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix NULL pointer dereference in nvmet_execute_identify_nslist() When a host issues an Identify command with CNS 07h (Active Namespace ID List for a specific I/O Command Set), nvmet_execute_identify_nslist() is called with match_css set. The command-set filter dereferences req->ns, but this handler never calls nvmet_req_find_ns(), so req->ns is always NULL (nvmet_req_init() resets it to NULL). As soon as an enabled namespace with an NSID greater than the requested value exists, req->ns->csi dereferences a NULL pointer and oopses. Besides the crash, the comparison is logically wrong: to filter the list by command set it must test the command set of the namespace being iterated, not a single fixed value. Use the loop variable ns->csi.	N/A	More Details

CVE-2026-80814	In the Linux kernel, the following vulnerability has been resolved: rndis_host: add overflow check in rndis_rx_fixup() Add an overflow check to ensure that data_offset + data_len + 8 does not wrap, which would enable an OOB read of the USB data buffer.	N/A	More Details
CVE-2026-80815	In the Linux kernel, the following vulnerability has been resolved: ALSA: scarlett2: Use a private URB for the notification endpoint scarlett2_init_notify() used mixer->urb, which snd_usb_mixer_status_create() allocates for the UAC2 status interrupt endpoint and mixer.c manages. On a device with that endpoint, the "already in use" check fires on the status URB and returns 0 for success without doing anything. No notification URB is submitted, and cmd_done is left zeroed because it is initialised past that check and nowhere else. scarlett2_usb_init() then issues SCARLETT2_USB_INIT_1 and wait_for_completion_timeout() would crash adding to the zeroed wait.head. Use a separate URB in scarlett2_data, as done for FCP, and initialise cmd_done in scarlett2_init_private(). mixer.c was also freeing the URB in snd_usb_mixer_free() and resubmitting it in snd_usb_mixer_activate(), so scarlett2 must now do both: add scarlett2_cleanup_urb(), called from private_free and private_suspend, and a private_resume callback to re-establish the URB after resume. scarlett2_init_notify() is reached from there, and the URB kill path in scarlett2_notify() completes cmd_done, leaving a stale count that would satisfy the next command's wait before the device ACKs. Use reinit_completion() to clear it. Also free the URB if the transfer buffer allocation fails, and both if usb_submit_urb() fails. Move scarlett2_init_notify() up next to scarlett2_cleanup_urb() so scarlett2_init_private() can reference it without a forward declaration.	N/A	More Details
CVE-2026-80816	In the Linux kernel, the following vulnerability has been resolved: ALSA: FCP: Use a private URB for the notification endpoint fcp_init_notify() used mixer->urb, which snd_usb_mixer_status_create() allocates for the optional UAC2 status interrupt endpoint and mixer.c kills, resubmits and frees. On a device with that endpoint, fcp_init_notify()'s "already set up" early return fires on the status URB and returns success without doing anything. No FCP notification URB is submitted, and cmd_done is left zeroed because it is initialised past that early return and nowhere else. fcp_init() then issues init1_opcode and wait_for_completion_timeout() would crash adding to the zeroed wait.head. fcp_cleanup_urb() would also kill and free mixer.c's status URB. Use a separate URB in fcp_data, and initialise cmd_done in fcp_init_private() where fcp_data is allocated. fcp_init_notify() is reached again after suspend via fcp_reinit(), and the URB kill path in fcp_notify() completes cmd_done, leaving a stale count that would satisfy the next command's wait before the device ACKs. Use reinit_completion() to clear it.	N/A	More Details
CVE-2026-80817	In the Linux kernel, the following vulnerability has been resolved: iommu/iommufd: Fix NULL pointer deref in iommufd_ioas_change_process when racing with iopt_map_file_pages iommufd_ioas_change_process() iterates every IOAS area while only holding every IOAS iova_rwsem, so it assumes every area has a non-NULL pages pointer. That assumption can be false when it runs concurrently with iopt_map_file_pages(). iopt_map_pages() executes in two phases. It first creates the area and inserts it into the interval tree under iova_rwsem, with area->pages still NULL. It then drops iova_rwsem and later fills area->pages under domains_rwsem. This leaves a window between area creation and area->pages fill where a concurrent iommufd_ioas_change_process() can observe the area and dereference a NULL area->pages pointer, leading to a NULL pointer dereference: BUG: kernel NULL pointer dereference, address: 00000000000000c0 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 4b655067 P4D 4b655067 PUD 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 0 UID: 0 PID: 11841 Comm: syz.1.628 Not tainted 7.1.0 #3 PREEMPT(full) Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:iommufd_ioas_change_process+0x419/0xd50 drivers/iommu/iommufd/ioas.c:538 Code: 48 89 c3 48 85 c0 0f 84 cc 00 00 00 e8 10 f5 cb fd 48 8d 7b 68 e8 a7 b5 eb fd 48 8b 6b 68 48 8d bd c0 00 00 00 e8 17 b2 eb fd <8b> ad c0 00 00 00 bf 01 00 00 00 89 ee e8 85 ef cb fd 83 fd 01 74 RSP: 0018:ffffc90015c17d28 EFLAGS: 00010246 RAX: ffff8880186d5328 RBX: ffff88801d25e240 RCX: 0000000080000000 RDX: 00000000000002d7 RSI: ffffffff83ba9e10 RDI: 00000000000000c0 RBP: 0000000000000000 R08: ffffffff8e781eb8 R09: 0000000000000000 R10: 00000000000000c0 R11: ffffffff83ba9e29 R12: ffff88802e216008 R13: ffff88802e216000 R14: 0000000000000001 R15: 0000000000000000 FS: 00007f4aea3f66c0(0000) GS:ffff8880b1fa1000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000000000c0 CR3: 000000004b75c000 CR4: 0000000000350ef0 Call Trace: <TASK> iommufd_fops_ioctl+0x287/0x400 drivers/iommu/iommufd/main.c:533 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x120/0x170 fs/ioctl.c:583 x64_sys_call+0x1092/0x1fb0 arch/x86/include/generated/asm/syscalls_64.h:17 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x10a/0x680 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f4aec1a82bd Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 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 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f4aea3f6018 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 00007f4aec436090 RCX: 00007f4aec1a82bd RDX: 0000200000000180 RSI: 0000000000003b92 RDI: 0000000000000003 RBP: 00007f4aec250295 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f4aec436128 R14: 00007f4aec436090 R15: 00007ffd04ef23e0 </TASK> Modules linked in: CR2: 00000000000000c0 ---[end trace 0000000000000000]--- RIP: 0010:iommufd_ioas_change_process+0x419/0xd50 drivers/iommu/iommufd/ioas.c:538 Code: 48 89 c3 48 85 c0 0f 84 cc 00 00 00 e8 10 f5 cb fd 48 8d 7b 68 e8 a7 b5 eb fd 48 8b 6b 68 48 8d bd c0 00 00 00 e8 17 b2 eb fd <8b> ad c0 00 00 00 bf 01 00 00 00 89 ee e8 85 ef cb fd 83 fd 01 74 RSP: 0018:ffffc90015c17d28 EFLAGS: 00010246 RAX: ffff8880186d5328 RBX: ffff88801d25e240 RCX: 0000000080000000 RDX: 00000000000002d7 RSI: ffffffff83ba9e10 RDI:	N/A	More Details

	00000000000000c0 RBP: 0000000000000000 R08: ffffffff8e781eb8 R09: 0000000000000000 R10: 00000000000000c0 R11: ffffffff83ba9e29 R12: ffff88802e216008 R13: ffff88802e216000 R14: 0000000000000001 R15: 0000000000000000 FS: 00007f4aea3f66c0(000 ---truncated---		
CVE-2026-80818	In the Linux kernel, the following vulnerability has been resolved: iommu/tegra241-cmdqv: Fix CMD_SYNC use-after-free on teardown arm_smmu_impl_remove() is registered as a devres action in arm_smmu_impl_probe(), before arm_smmu_init_queues() allocates smmu->cmdq.q.base. On a devres unwind, whether a failed probe or an unbind, the queue is freed first and arm_smmu_impl_remove() then runs tegra241_cmdqv_remove_vintf(), whose VINTF deinit issues a CMD_SYNC on the freed memory. Observed during testing with a QEMU hack that makes the VCMDQ fail to enable, so the impl reset fails and probe aborts into the devres unwind: platform NVDA200C:00: tegra241_cmdqv: VINTF0: VCMDQ0/LVCMDQ0: failed to enable, STATUS=0x00000000 platform NVDA200C:00: tegra241_cmdqv: VINTF0: VCMDQ0/LVCMDQ0: GERRORN=0x0, GERROR=0x4, CONS=0x0 platform NVDA200C:00: tegra241_cmdqv: VINTF0: VCMDQ0/LVCMDQ0: uncleared error detected, resetting arm-smmu-v3 arm-smmu-v3.0.auto: failed to reset impl arm-smmu-v3 arm-smmu-v3.0.auto: probe with driver arm-smmu-v3 failed with error -110 Unable to handle kernel paging request at virtual address ffff8000891e0098 ... Internal error: Oops: 0000000096000047 [#1] SMP ... Call trace: arm_smmu_cmdq_issue_cmdlist+0x320/0x6fc (P) tegra241_vcmdq_hw_deinit+0x98/0x168 tegra241_vintf_hw_deinit+0x5c/0x1b0 tegra241_cmdqv_remove_vintf+0x34/0xec tegra241_cmdqv_remove+0x40/0x9c arm_smmu_impl_remove+0x20/0x30 devm_action_release+0x14/0x20 devres_release_all+0xa8/0x110 device_unbind_cleanup+0x18/0x84 really_probe+0x1f0/0x29c Drop the VINTF deinit from tegra241_cmdqv_remove_vintf() so the unwind no longer touches the freed queue. Quiesce the VINTFs earlier instead. Add a device_disable() impl op and run it from arm_smmu_disable_action() while the CMDQ is still up. That handles a live unbind. A failed reset is already handled because tegra241_vintf_hw_init() deinits the VINTF on its own error path. tegra241_cmdqv_remove_vintf() is also used by the iommufd viommu destroy path, so quiesce there too.	N/A	More Details
CVE-2026-80819	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: take rfcomm_mutex for the deferred setup accept rfcomm_sock_recvmsg() completes a deferred setup by calling rfcomm_dlc_accept() without holding any RFCOMM lock: if (test_and_clear_bit(RFCOMM_DEFER_SETUP, &d->flags)) { rfcomm_dlc_accept(d); return 0; } and rfcomm_dlc_accept() dereferences the session on its first line: struct sock *sk = d->session->sock->sk; Every other path that touches d->session runs under rfcomm_mutex: rfcomm_dlc_open(), rfcomm_dlc_close(), rfcomm_dlc_exists(), rfcomm_dlc_send_rpn(), and the RFCOMM thread through rfcomm_process_sessions(). rfcomm_connect_ind() is even documented as "called under rfcomm_lock()". This call site is the only one that skips it. The RFCOMM_DEFER_SETUP bit looks like it serialises the accept against teardown, since __rfcomm_dlc_close() returns early when it wins the test_and_clear. But rfcomm_recv_disc() forces the state first: d->state = BT_CLOSED; __rfcomm_dlc_close(d, err); and the early return only covers BT_CONNECT, BT_CONFIG, BT_OPEN and BT_CONNECT2. With the state already BT_CLOSED that switch does not match, the bit is never consulted, and __rfcomm_dlc_close() falls through to rfcomm_dlc_unlink(), which sets d->session = NULL. So a remote DISC on a deferred dlc clears the session while leaving RFCOMM_DEFER_SETUP set. The next recvmsg() then passes the test_and_clear and dereferences a NULL session. No timing window is needed: once the DISC has been processed, the dereference is unconditional. Give rfcomm_dlc_accept() the same shape as rfcomm_dlc_open() and rfcomm_dlc_close(): an exported wrapper that takes rfcomm_mutex and re-checks the session, around a __rfcomm_dlc_accept() that the two in-core callers, which already hold the mutex, keep using. Reproduced on a KASAN + PROVE_LOCKING kernel with a BR/EDR peer emulated over /dev/vhci: the peer brings up an ACL link, opens L2CAP on the RFCOMM PSM, starts a session, opens a dlc on a channel bound with BT_DEFER_SETUP, and sends DISC after the socket is accepted. recv() on the accepted socket then hits: Oops: general protection fault KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] RIP: 0010:rfcomm_dlc_accept+0x54/0x350 Call Trace: rfcomm_sock_recvmsg+0x1cd/0x230 sock_recvmsg+0x166/0x1c0 __sys_recvfrom+0x20d/0x300 0x10 is the offset of sock in struct rfcomm_session. With this patch the same run completes with recv() returning 0 and no report, and lockdep stays quiet, confirming rfcomm_mutex is still taken before lock_sock on this path as it is on the thread side.	N/A	More Details
CVE-2026-80820	In the Linux kernel, the following vulnerability has been resolved: xfs: don't livelock in scrub on a circular unlinked list LOLLM points out that online fsck can livelock if an unlinked inode list contains a loop. Use a bitmap to detect cycles.	N/A	More Details
CVE-2026-80822	In the Linux kernel, the following vulnerability has been resolved: mailbox: mchp-ipc-sbi: Add null check for devm_kasprintf() Add a check to see if devm_kasprintf() is not NULL in mchp_ipc_get_cluster_aggr_irq(), returning -ENOMEM if the function failed.	N/A	More Details
CVE-2026-80831	In the Linux kernel, the following vulnerability has been resolved: crypto: mxs-dcp - fix source scatterlist length access mxs_dcp_aes_block_crypt() uses sg_dma_len() without mapping the source scatterlist with dma_map_sg() first. Therefore, sg_dma_len() is invalid and could return zero or a stale DMA length, causing encryption and decryption to process the wrong number of bytes when CONFIG_NEED_SG_DMA_LENGTH=y. Use the original scatterlist length instead.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: nfc: st21nfca: validate ATR_REQ length against the received frame st21nfca_tm_recv_atr_req() checks that the received ATR_REQ frame is at least ST21NFCA_ATR_REQ_MIN_SIZE and that the self-declared atr_req->length is at least sizeof(struct		

CVE-2026-80823	st21nfca_atr_req), but never checks that atr_req->length does not exceed the actual received length (skb->len). st21nfca_tm_send_atr_res() then trusts the declared length: gb_len = atr_req->length - sizeof(struct st21nfca_atr_req); ... memcpy(atr_res->gbi, atr_req->gbi, gb_len); so an RF peer that sends a short frame but sets atr_req->length larger than the frame makes gb_len exceed the general bytes actually present, and the memcpy reads out of bounds past the received skb. Those bytes are placed in the ATR_RES and sent back to the peer (kernel-memory disclosure to a proximity attacker); a larger declared length is an out-of-bounds read (DoS). Reject frames whose declared length exceeds the received length. The adjacent nfc_tm_activated() path in the same function already derives its general-bytes length from skb->len rather than the declared field. Found by 0sec (https://0sec.ai) using automated source analysis; the missing bound is evident from source. Compile-tested.	N/A	More Details
CVE-2026-80824	In the Linux kernel, the following vulnerability has been resolved: usb: usbfs: fix use-after-free of usb_device in usbdev_release() usbdev_release() drops its reference to the struct usb_device before draining the list of completed async URBs, but that drain path reads back through the same object: free_async() calls dec_usb_memory_use_count() for any URB whose buffer came from the usbfs mmap() region, and its first statement is bus_to_hcd(ps->dev->bus). After a disconnect the usbfs reference can be the last one, in which case usb_put_dev() frees the device and the subsequent loop reads offset 80 of freed memory and uses the result as a struct usb_hcd *, which hcd_buffer_free_pages() then dereferences. This is reachable by an unprivileged process that has read/write access to a /dev/bus/usb node: mmap() the fd, submit one URB with a buffer inside the mapping, wait for the device to be unplugged, then munmap() and close(). It reproduces on every attempt rather than being a race, because a live MAP_SHARED vma holds a reference on the struct file, so usbdev_release() cannot run until the last vma is gone and the freeing branch of dec_usb_memory_use_count() is always taken. BUG: KASAN: slab-use-after-free in dec_usb_memory_use_count+0x3ae/0x410 Read of size 8 at addr ffff8880122ee050 by task poc/769 CPU: 1 UID: 1000 PID: 769 Comm: poc Tainted: G B 6.12.94 #3 Call Trace: dec_usb_memory_use_count+0x3ae/0x410 free_async+0x2aa/0x4f0 usbdev_release+0x375/0x460 __fput+0x3ea/0xb50 __x64_sys_close+0x86/0x100 Allocated by task 11: usb_alloc_dev+0x55/0xd90 hub_event+0x2524/0x43d0 Freed by task 769: kfree+0x121/0x360 device_release+0xd2/0x280 usb_put_dev+0x23/0x30 usbdev_release+0x2d8/0x460 Release the device reference after the drain loop instead. Nothing between the two points requires it to have been dropped.	N/A	More Details
CVE-2026-80825	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: ensure tx headroom in usb_sdio_tx_prepare_skb mt7925_usb_sdio_tx_prepare_skb() pushes a TX descriptor and a USB header onto every skb and assumes the headroom for them is already there. That holds for locally generated traffic, where mac80211 reserves hw->extra_tx_headroom, but forwarded frames are sent through ieee80211_8023_xmit(), which does not reserve it. Bridge a wired interface to an mt7925u AP and the first forwarded frame that arrives short panics the kernel: skbuff: skb_under_panic: len:415 put:4 tail:0x19b end:0x640 dev:wlan1 kernel BUG at net/core/skbuff.c:212! Call trace: skb_panic+0x58/0x60 (P) skb_push+0x58/0x60 mt7925_usb_sdio_tx_prepare_skb+0xf8/0x1b8 [mt7925_common] mt76u_tx_queue_skb+0xa0/0x1f8 [mt76_usb] __mt76_tx_queue_skb+0x54/0xe8 [mt76] mt76_txq_schedule.part.0+0x204/0x478 [mt76] mt76_txq_schedule_all+0x50/0x80 [mt76] mt792x_tx_worker+0x68/0x100 [mt792x_lib] __mt76_worker_fn+0x84/0x150 [mt76] Whether a given setup hits it depends on how much headroom the ingress netdev leaves in its rx skbs. Reproduced on a Raspberry Pi 5 bridging onboard ethernet to a Netgear A9000; originally reported on an MT7986 router running OpenWrt. Nick Morrow's testing on a Pi 4 (bcmgenet), which leaves more headroom, helped narrow the trigger to the ingress path. The same bug was fixed on mt7921 by commit 98c4d0abf5c4 ("mt76: mt7921: don't assume adequate headroom for SDIO headers"), but mt7925 was copied from mt7921 without the fix. Add the same guard here.	N/A	More Details
CVE-2026-80826	In the Linux kernel, the following vulnerability has been resolved: USB: c67x00: fix use-after-free in c67x00_add_iso_urb() When TD creation fails for the last packet of an isochronous URB, c67x00_add_iso_urb() gives the URB back before updating the endpoint scheduling state. c67x00_giveback_urb() frees the URB private data, and the completion callback may release the final URB reference. The following accesses to urbp->ep_data, urb->interval, and urbp->cnt can therefore use freed memory. Update next_frame and cnt before giving back the failed final packet, making the giveback the last operation that uses the URB and its private data.	N/A	More Details
CVE-2026-80827	In the Linux kernel, the following vulnerability has been resolved: USB: serial: option: fix slab OOB read in interrupt URB callback The interrupt URB buffer is allocated in setup_port_interrupt_in() based on the endpoint's wMaxPacketSize: buffer_size = usb_endpoint_maxp(epd); port->interrupt_in_buffer = kmalloc(buffer_size, GFP_KERNEL); When a USB device declares wMaxPacketSize = 8 on its interrupt IN endpoint, the buffer is allocated from kmalloc-8 cache (exactly 8 bytes). If the device sends a short packet (actual_length < wMaxPacketSize), the URB completes with status == 0 and the callback proceeds to read: data[sizeof(struct usb_ctrlrequest)] which evaluates to data[8], accessing 1 byte beyond the allocated 8-byte buffer. This results in a slab out-of-bounds read. Fix this by adding the missing bounds check: first verify that the actual length is large enough to contain the struct usb_ctrlrequest header before accessing req_pkt->bRequestType and req_pkt->bRequest, and then verify that there is an additional byte for the modem signal state before reading data[sizeof(struct usb_ctrlrequest)] inside the conditional. Use sizeof(*req_pkt) instead of sizeof(struct usb_ctrlrequest) for consistency. [johan: use dev_err(); split signals declaration and initialisation]	N/A	More Details

CVE-2026-80828	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Complete cleanup after system-resume errors A failed system resume can leave the card unusable until reboot. usb_audio_resume() jumps to err_out when snd_usb_pcm_resume() or snd_usb_mixer_resume() fails. The error path skips the out: block, which restores D0 and decrements chip->num_suspended_intf. The card stays in SNDRV_CTL_POWER_D3hot, so later control access blocks in snd_power_ref_and_wait(). USB core logs an interface resume callback error. It does not retry that callback, so a later callback cannot complete the skipped cleanup. usb_audio_suspend() increments num_suspended_intf before returning success. A system-resume callback must consume the system-suspend count even if a component resume fails. Otherwise, the stranded count skews later suspend and resume cycles. Do not apply this cleanup to runtime-resume errors. Runtime PM can retry -EAGAIN or -EBUSY without another suspend callback. The count must continue to describe that suspended interface. Other runtime-resume errors latch runtime_error in the PM core and do not cause an immediate callback retry. Both parts of the system-resume error path are longstanding. Commit 88a8516a2128a ("ALSA: usbaudio: implement USB autosuspend") introduced err_out past the D0 restore. Commit 862b2509d157c ("ALSA: usb-audio: Fix inconsistent card PM state after resume") later moved num_suspended_intf-- into the out: block. The error path now skips both operations. No third-party code is needed to reach the error path. snd_usb_mixer_resume() ends in snd_usb_mixer_activate(), which returns the result of usb_submit_urb() for devices that have a mixer status URB. Its mixer->private_resume hook can also fail through scarlett2_init_notify(). snd_usb_pcm_resume() issues a SET_CUR request to a UAC3 power domain. It can return -EPIPE or -EIO when the device stalls the request. Route a component error through out: only when system_suspend is nonzero. Continue to return runtime-resume errors through err_out. Later component resume stages remain skipped. The original error still reaches USB core. A later transfer can fail if the device did not recover. I reproduced the system-resume failure on an Audient iD14 MkI with an out-of-tree diagnostic mixer resume hook. An injected -EIO on the unpatched core left control readers in uninterruptible sleep in snd_power_ref_and_wait() until a reboot. With this patch, the same failure restored control access. A second system suspend and resume also succeeded after I disabled fault injection.	N/A	More Details
CVE-2026-80829	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: fix OOB write in snd_usbmidi_novation_output() snd_usbmidi_novation_output() lays out a two-byte header at transfer_buffer[0..1] and passes &transfer_buffer[2] together with a length of ep->max_transfer - 2 to snd_rawmidi_transmit(): count = snd_rawmidi_transmit(ep->ports[0].substream, &transfer_buffer[2], ep->max_transfer - 2); ep->max_transfer comes from the output endpoint's wMaxPacketSize via usb_maxpacket(). A malformed or malicious device can advertise a bulk OUT endpoint with a wMaxPacketSize of 1 - the USB core only clamps this value downwards - so ep->max_transfer becomes 1 and the count argument becomes -1. snd_rawmidi_transmit() passes the negative count on to __snd_rawmidi_transmit_peek(), where "if (count1 > count) count1 = count" leaves count1 negative; get_aligned_size() keeps it negative for a byte-stream substream, so the following memcpy(buffer, ..., count1) runs with a (size_t)-1 length and writes far past the transfer buffer, which was allocated with usb_alloc_coherent(ep->max_transfer). This is the same class of bug that was fixed for snd_usbmidi_akai_output() in commit 0970274613fb ("ALSA: usb-audio: fix OOB write in snd_usbmidi_akai_output()"); the novation output routine was left unguarded. Bail out when the endpoint cannot hold the two-byte header plus at least one payload byte.	N/A	More Details
CVE-2026-80830	In the Linux kernel, the following vulnerability has been resolved: usb: core: Add lock to usb_wakeup_notification() Add a spin lock to usb_wakeup notification to prevent a race condition with dereferencing freed memory. This could be hit by the xHCI driver as it calls this function from an IRQ and could race with the hub_disconnect() function, which properly grabs this lock to protect the state of the device.	N/A	More Details
CVE-2026-80854	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_tcm: keep port count until LUN teardown completes tcm_usbg_drop_nexus() permits session removal once tpg_port_count reaches zero. However, usbg_port_unlink() currently decrements that count from the fabric_pre_unlink() callback, before core_dev_del_lun() waits for active se_lun references to drain. If removal of the last LUN races a nexus removal, the latter can observe a zero port count and call target_remove_session(). This frees sess_cmd_map while an in-flight struct usbg_cmd, including its work item, can still be accessed. Overlapping the last-LUN unlink with nexus removal reproduces this lifetime violation as a DEBUG_OBJECTS "free active" warning for usbg_cmd_work, followed by a target-core BUG/Oops. The generic target-core unlink path has no callback after core_dev_del_lun() completes. Add an optional fabric_post_unlink() callback and use it for the f_tcm port count. The count now remains nonzero until core_dev_del_lun() has finished draining active LUN references, preventing nexus removal from freeing the session during command completion.	N/A	More Details
CVE-2026-80855	In the Linux kernel, the following vulnerability has been resolved: fuse: fix invalidate lock leak on open O_TRUNC DAX failure fuse_open() takes filemap_invalidate_lock() for a DAX truncate (dax_truncate = true) and releases it before the out_inode_unlock label. But when fuse_dax_break_layouts() fails, the goto out_inode_unlock skips the unlock and leaks the rwsem, so any later fault or truncate on the file stalls on the stale lock. fuse_dax_break_layouts() can fail with -ERESTARTSYS when a signal interrupts the wait for busy DAX pages to drain: open("file", O_RDWR | O_TRUNC) └─ fuse_open() ├─ filemap_invalidate_lock() # dax_truncate └─ fuse_dax_break_layouts() └─ dax_break_layout() └─ wait_page_idle() # TASK_INTERRUPTIBLE └─ fuse_wait_dax_page() # unlock, schedule, re-lock └─ signal → -ERESTARTSYS goto out_inode_unlock # <- lock leaked Fix this by moving filemap_invalidate_unlock() below the label so that all error paths release the lock, and rename the label to out_unlock as it now covers more than just the inode lock.	N/A	More Details

CVE-2026-80856	In the Linux kernel, the following vulnerability has been resolved: fuse: fix invalidate lock leak on setattr writeback failure fuse_do_setattr() takes filemap_invalidate_lock() for a DAX truncate (fault_blocked = true) and releases it at the out:/error: labels. But when a writeback flush is also needed, a write_inode_now() failure returns directly and leaks the lock, so any later fault or truncate on the file stalls on the stale rwsem. For example, truncate(2) on a setuid file reaches fuse_do_setattr() with both ATTR_SIZE and ATTR_MODE set: truncate(2) └─ do_truncate() ├─ dentry_needs_remove_privs() # S_ISUID └─ notify_change() # KILL_SUID -> ATTR_MODE └─ fuse_setattr() # no killpriv: │ # ia_valid |= ATTR_MODE └─ fuse_do_setattr() ├─ filemap_invalidate_lock() # IS_DAX && is_truncate └─ write_inode_now() # is_wb && ATTR_MODE └─ if (err) # e.g. daemon -> -EIO return err # <- lock leaked Fix this by adding an unlock label that releases the lock before returning the error, and use it for the fuse_dax_break_layouts() failure path as well.	N/A	More Details
CVE-2026-80884	In the Linux kernel, the following vulnerability has been resolved: ntb: Store original DMA address for future release The DMA API requires that dma_free_attrs receive the exact dma_handle originally returned by the allocation function. Do not modify it.	N/A	More Details
CVE-2026-80876	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Fix event length with forced 8-byte alignment When RB_FORCE_8BYTE_ALIGNMENT is true, rb_calculate_event_length() reserves the space of event->array[0] for placing the data length and rb_update_event() stores the data length in event->array[0] accordingly. As a result the whole event length will add extra 4 bytes for sizeof(event.array[0]) unconditionally. But ring_buffer_event_length() only subtracts the sizeof(event->array[0]) for events larger than RB_MAX_SMALL_DATA + sizeof(event->array[0]). As a result, small events on architectures with RB_FORCE_8BYTE_ALIGNMENT=true report a data length that is 4 bytes larger than expected. To fix it, add the RB_FORCE_8BYTE_ALIGNMENT as a condition to subtract the size of that length field whenever RB_FORCE_8BYTE_ALIGNMENT is true. This issue is observed in a riscv64 kernel with CONFIG_HAVE_64BIT_ALIGNED_ACCESS set to y, when we run ftrace selftest trace_marker_raw.tc, we get the weird log: for cases where the id is 1..100, the number of data field is 8*N, but once id exceeds 100, the number of data field becomes 8*N+4: # 1 buf: 58 00 00 00 80 5e d1 63 (number of data field is 8*1) ... # a buf: 58 ... (number of data field is 8*2) ... # 64 buf: 58 ... (number of data field is 8*13) # 65 buf: 58 ... (number of data field is 8*13+4) After applying this change, the number of data field keeps being 8*N+4 consistently.	N/A	More Details
CVE-2026-80877	In the Linux kernel, the following vulnerability has been resolved: afs: Fix vllist leak Fix a leak of the new vllist in afs_update_cell() in the event that it is an empty list (nr_servers == 0), in which case the old list isn't displaced unless the old list is also empty.	N/A	More Details
CVE-2026-80878	In the Linux kernel, the following vulnerability has been resolved: afs: Fix leak of ungot volume Fix afs_lookup_volume_rcu() so that it doesn't leak a dying volume if afs_try_get_volume() fails.	N/A	More Details
CVE-2026-80879	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix circular locking dependency in ocfs2_dio_end_io_write A circular locking dependency involves INODE_ALLOC_SYSTEM_INODE, EXTENT_ALLOC_SYSTEM_INODE, and ORPHAN_DIR_SYSTEM_INODE. 1. ocfs2_mknod() acquires INODE_ALLOC then EXTENT_ALLOC. 2. ocfs2_dio_end_io_write() acquires EXTENT_ALLOC for unwritten extents, then ORPHAN_DIR via ocfs2_del_inode_from_orphan() while still holding EXTENT_ALLOC. 3. ocfs2_wipe_inode() acquires ORPHAN_DIR then INODE_ALLOC via ocfs2_remove_inode. Break the cycle in ocfs2_dio_end_io_write() by freeing the allocation contexts (releasing EXTENT_ALLOC) before acquiring ORPHAN_DIR. WARNING: possible circular locking dependency detected -- is trying to acquire lock: ffff8881e78b33a0 (&ocfs2_sysfile_lock_key[INODE_ALLOC_SYSTEM_INODE]) {+.+.}-{4:4}, at: ocfs2_evict_inode+0x1539/0x43b0 fs/ocfs2/inode.c:1299 but task is already holding lock: ffff8881e78b4fa0 (&ocfs2_sysfile_lock_key[ORPHAN_DIR_SYSTEM_INODE]){+.+.}-{4:4}, at: ocfs2_evict_inode+0xe97/0x43b0 fs/ocfs2/inode.c:1299 the existing dependency chain (in reverse order) is: -> #2 (&ocfs2_sysfile_lock_key[ORPHAN_DIR_SYSTEM_INODE]){+.+.}-{4:4}: inode_lock include/linux/fs.h:1029 [inline] ocfs2_del_inode_from_orphan+0x12e/0x7a0 fs/ocfs2/namei.c:2728 ocfs2_dio_end_io+0xf9c/0x1370 fs/ocfs2/aops.c:2418 dio_complete+0x25b/0x790 fs/direct-io.c:281 -> #1 (&ocfs2_sysfile_lock_key[EXTENT_ALLOC_SYSTEM_INODE]){+.+.}-{4:4}: inode_lock include/linux/fs.h:1029 [inline] ocfs2_reserve_suballoc_bits+0x16d/0x4840 fs/ocfs2/suballoc.c:882 ocfs2_reserve_new_metadata_blocks+0x415/0x9a0 fs/ocfs2/suballoc.c:1078 ocfs2_mknod+0x10f3/0x2260 fs/ocfs2/namei.c:351 -> #0 (&ocfs2_sysfile_lock_key[INODE_ALLOC_SYSTEM_INODE]){+.+.}-{4:4}: __lock_acquire+0x15a5/0x2cf0 kernel/locking/lockdep.c:5237 lock_acquire+0x106/0x350 kernel/locking/lockdep.c:5868 down_write+0x96/0x200 kernel/locking/rwsem.c:1625 inode_lock include/linux/fs.h:1029 [inline] ocfs2_remove_inode fs/ocfs2/inode.c:733 [inline] ocfs2_wipe_inode fs/ocfs2/inode.c:896 [inline] ocfs2_delete_inode fs/ocfs2/inode.c:1157 [inline] ocfs2_evict_inode+0x1539/0x43b0 fs/ocfs2/inode.c:1299 Chain exists of: &ocfs2_sysfile_lock_key[INODE_ALLOC_SYSTEM_INODE] --> &ocfs2_sysfile_lock_key[EXTENT_ALLOC_SYSTEM_INODE] --> &ocfs2_sysfile_lock_key[ORPHAN_DIR_SYSTEM_INODE] Possible unsafe locking scenario: CPU0 CPU1 ---- ---- lock(&ocfs2_sysfile_lock_key[ORPHAN_DIR_SYSTEM_INODE]); lock(&ocfs2_sysfile_lock_key[EXTENT_ALLOC_SYSTEM_INODE]); lock(&ocfs2_sysfile_lock_key[ORPHAN_DIR_SYSTEM_INODE]); lock(&ocfs2_sysfile_lock_key[INODE_ALLOC_SYSTEM_INODE]); *** DEADLOCK ***	N/A	More Details

CVE-2026-80880	In the Linux kernel, the following vulnerability has been resolved: IB/mlx5: Properly support implicit ODP rereg_mr Due to all the child mkeys in the implicit ODP configuration we cannot change anything in place for the parent mkey. Instead the whole thing needs to be rebuilt if any change is requested. If the user does not specify a translation then force the implicit values which will then fall through the logic into mlx5_ib_reg_user_mr() to allocate a completely new MR. Since implicit children were also touching the mr->pd, this removes another case where the access was racy.	N/A	More Details
CVE-2026-80881	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix buffer head management in ocfs2_read_blocks() In ocfs2_read_blocks(), caller should't assume that buffer head returned by 'sb_getblk()' is exclusively owned and so 'put_bh()' always drops b_count from 1 to 0. If it is not so, buffer head remains on hold and likely to be returned by the next call to 'sb_getblk()' unchanged - that is, with BH_Uptodate bit set even if it has failed validation previously, thus allowing to insert that buffer head into OCFS2 metadata cache and submit it to upper layers. To avoid such a scenario, BH_Uptodate should be cleared immediately after 'validate()' callback has detected some data inconsistency.	N/A	More Details
CVE-2026-80882	In the Linux kernel, the following vulnerability has been resolved: crypto: tegra - Return ENOMEM when input buffer allocation fails for ccm Ensure the ENOMEM error value is set when the input buffer allocation fails in tegra_ccm_do_one_req.	N/A	More Details
CVE-2026-80883	In the Linux kernel, the following vulnerability has been resolved: drm/tegra: gr2d/gr3d: Initialize address register map before HOST1X client is registered The host1x_client_register() function is called just prior to register map initialization loop, making the device available to userspace. This may result in userspace attempting to submits a job before the register map is initialized. Address this by moving register initialization before host1x client registration.	N/A	More Details
CVE-2026-80885	In the Linux kernel, the following vulnerability has been resolved: afs: Fix uncancelled rxrpc OOB message handler Fix AFS to cancel its OOB message processing (typically to respond to security challenges). Also move OOB message processing to afs_wq so that it's also waited for and make the OOB handler just return if the net namespace is no longer live.	N/A	More Details
CVE-2026-80874	In the Linux kernel, the following vulnerability has been resolved: arm64: dts: renesas: ironhide: Describe inline ECC carveouts The DBSC5 DRAM controller protects DRAM content using inline ECC. The inline ECC utilizes areas of DRAM for its operation, which are in the DRAM address range, but must not be accessed or modified. Describe the inline ECC carveout areas used by the DBSC5 controller on this hardware as reserved-memory, which must not be accessed. Include DRAM areas which are unprotected by ECC as well, those are parts of the DRAM which directly precede the ECC carveout. In case of high DRAM utilization, unless the inline ECC carveouts are properly reserved, Linux may use and corrupt the memory used by the DBSC5 DRAM controller for inline ECC, which would lead to the system becoming unstable.	N/A	More Details
CVE-2026-80886	In the Linux kernel, the following vulnerability has been resolved: serial: msm: Disable DMA for kernel console UART At the moment, concurrent writes from userspace and the kernel to the console can trigger a race condition that results in an infinite loop of the same messages printed over and over again. This is most likely to happen during system startup or shutdown when the init system starts/stops a large number of system services that interact with various kernel code. When userspace writes to the TTY device, the driver initiates an asynchronous DMA transfer and releases the port lock. At the same moment, the kernel printk path might grab the port lock and re-configure the UART controller for PIO, without waiting for the DMA operation to complete. It seems like this collision results in zero progress being reported for the DMA engine, so the same text is printed to the console over and over again. For the kernel console, we want a reliable output path that will be functional even during crashes etc. So rather than implementing complex code to synchronize the kernel console write routines with the userspace DMA write routines, simply disable DMA for the console UART instance. Similar checks exist in many other serial drivers, e.g. 8250_port.c, imx.c, sh-sci.c etc.	N/A	More Details
CVE-2026-18745	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-50553	Note Mark is an open-source note-taking application. Prior to version 0.19.5, Note Mark validates book and note slug values with the OpenAPI/huma tag pattern:"[a-z0-9-]+". huma compiles this with regexp.MustCompile(s.Pattern) and tests it with patternRe.MatchString(str), an UNANCHORED match. Because the pattern is not anchored (^...$), any string that merely CONTAINS one [a-z0-9-] substring passes validation. A slug such as ../../../../../tmp/escape is accepted and stored verbatim. The data-export CLI commands (note-mark migrate export and note-mark migrate export-v1) join these unsanitized slugs straight into the output path with path.Join / filepath.Join, then os.MkdirAll the directory and os.Create the note file. path.Join resolves the ../ segments, so the note content file is written OUTSIDE the configured export directory. The export process commonly runs as root (default in Docker / bare-metal admin usage), so this is a root-privilege arbitrary directory create + file write. This issue has been patched in version 0.19.5.	N/A	More Details
CVE-2026-53757	Emlog is an open source website building system. In versions 2.6.29 and prior, the emUnZip() function extracts all ZIP entries via ZipArchive::extractTo() without validating entry paths for ../ traversal sequences. Only the first entry's subdirectory structure is checked. An attacker can overwrite arbitrary files on the server filesystem, including config.php for immediate RCE. At time of publication, there are no publicly known	N/A	More Details

	patches.		
CVE-2026-53758	Emlog is an open source website building system. In versions 2.6.29 and prior, article content is processed by Parsedown without enabling safe mode, which means raw HTML including <script> tags embedded in Markdown is passed through unescaped. The output is rendered with no additional sanitization, resulting in stored XSS visible to all site visitors. At time of publication, there are no publicly known patches.	N/A	More Details
CVE-2026-53761	Frappe CRM is an open-source customer relationship management tool. Prior to version 1.73.0, there is an authentication bypass vulnerability via logged invitation keys in crm/api. This issue has been patched in version 1.73.0.	N/A	More Details
CVE-2026-57159	PJSIP is a free and open source multimedia communication library written in C. Prior to commit 673b978, a remote out-of-bounds read and write can occur in the SDP negotiator when the remote payload-type map maintenance feature is enabled. assign_pt_and_update_map() in pjmedia/src/pjmedia/sdp_neg.c uses payload-type numbers taken from a remote SDP offer or answer to index fixed-size internal tables without sufficient bounds validation, so a crafted remote SDP can cause memory access outside those tables. The practical impact is memory corruption and denial of service; code execution is not demonstrated. This path is only reached when PJMEDIA_SDP_NEG_MAINTAIN_REMOTE_PT_MAP is enabled. The default is disabled, so default builds are not affected; the feature is an interoperability option that integrating products may enable. This issue has been patched via commit 673b978.	N/A	More Details
CVE-2026-57160	PJSIP is a free and open source multimedia communication library written in C. Prior to commit d6a0e7f, a buffer overflow can occur in pjsip_generic_array_hdr_print() in pjsip/src/pjsip/sip_msg.c, the function that serializes generic array headers (such as Allow, Require, Supported, and Unsupported). Under certain output-buffer boundary conditions the function can write one byte past the end of the buffer. This is reachable mainly in applications that parse and re-serialize incoming SIP requests — for example a proxy, SBC, or B2BUA — where a remote peer can influence the serialized message. The out-of-bounds write is a single fixed byte; code execution and information disclosure are not demonstrated, and in typical pool-based allocations the byte falls within allocation slack. This issue has been patched via commit d6a0e7f.	N/A	More Details
CVE-2026-80875	In the Linux kernel, the following vulnerability has been resolved: ipvs: use parsed transport offset in TCP state lookup TCP state handling reparses the skb to find the TCP header. For IPv6 it uses sizeof(struct ipv6hdr), while the surrounding IPVS code already parsed the packet with ip_vs_fill_iph_skb() and has the real transport-header offset in iph.len. This makes TCP state handling look at the wrong bytes when an IPv6 packet carries extension headers. Use the parsed transport offset passed down from ip_vs_set_state() when reading the TCP header. For IPv4 and for IPv6 packets without extension headers, the passed offset matches the previous value.	N/A	More Details
CVE-2026-80873	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Write ESR_EL2 for injected nested SError exceptions kvm_inject_el2_exception() writes ESR_EL2 for synchronous exceptions but not for SError. enter_exception64() does not write ESR_ELx for any exception type, so the constructed syndrome is dropped. A guest L2 hypervisor taking a nested SError observes stale ESR_EL2. This affects both kvm_inject_nested_serror() and the EASE path in kvm_inject_nested_sea(). Write ESR_EL2 for except_type_serror, matching except_type_sync.	N/A	More Details
CVE-2026-80857	In the Linux kernel, the following vulnerability has been resolved: fuse: wait for FR_FINISHED on abort_on_kill to prevent use-after-free The abort_on_kill path in request_wait_answer() calls fuse_abort_conn() and returns without waiting for FR_FINISHED. If fuse_dev_do_write() is concurrently processing the same request (FR_LOCKED set), the caller frees req->args while it is still being accessed, causing a use-after-free. Fix this by jumping to the existing wait_event(FR_FINISHED) instead of returning early. The wait will not hang because fuse_abort_conn() ensures all requests are ended.	N/A	More Details
CVE-2026-85730	smol-toml is a small, fast, and correct TOML parser and serializer. Prior to 1.7.1, parse() can enter an infinite loop when a value inside an array or inline table is followed by a comment with no trailing newline. In src/util.ts, skipUntil() calls indexOfNewline(), receives -1 at the end of input, and resets the cursor to the beginning of the string instead of leaving the structure scan. The parser then hangs indefinitely and can consume a service's processing capacity when an application parses attacker-controlled TOML. This issue is fixed in version 1.7.1.	N/A	More Details
CVE-2026-80858	In the Linux kernel, the following vulnerability has been resolved: fuse: publish io-uring queues with release semantics fuse_uring_create_queue() initializes a fuse_ring_queue and then publishes the pointer into ring->queues[qid] with WRITE_ONCE() under the fch->lock. There are several readers that may concurrently be fetching that pointer locklessly and then deferencing it. WRITE_ONCE() doesn't ensure ordering of the queue's field initialization before the ring->queues[qid] pointer assignment. The queue must be published with smp_store_release() so the field initialization is guaranteed to happen before. Readers in paths where the read may happen concurrently with the store need to use READ_ONCE() because any race involving a plain access is undefined.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: fuse: fix missing barrier when checking io-uring readiness fuse_block_alloc() reads fch->initialized and then fch->io_uring. fch->io_uring is set before fch->initialized, ordered by the smp_wmb() in fuse_chan_set_intialized(), but fuse_block_alloc() has no		More

2026-80859	matching read barrier between the two loads. This may lead a CPU to observe fch->initialized=1 but fch->io_uring=0, and skip the check that blocks request allocation until the io-uring queues are ready. This can reintroduce the lock-order inversion deadlock that commit 3393ff964e0f prevents. Add an smp_rmb() barrier to pair with the smp_wmb() in fuse_chan_set_initialized() to prevent this.	N/A	Details
CVE-2026-80860	In the Linux kernel, the following vulnerability has been resolved: fuse: fix race between interrupt and resend After commit f8fce75fedf7 ("fuse: clear intr_entry in fuse_resend and fuse_remove_pending_req") the WARN_ON(!list_empty(&req->intr_entry)) in fuse_request_free() still triggers due to the following race: In request_wait_answer() if (test_bit(FR_SENT, &req->flags)) -> returns true In fuse_chan_resend() clear_bit(FR_SENT, &req->flags) In request_wait_answer() queue_interrupt(req) Fix by: - move clearing FR_SENT inside fpq->lock - move setting FR_PENDING inside fiq->lock - recheck FR_SENT after acquiring fiq->lock in fuse_dev_queue_interrupt()	N/A	More Details
CVE-2026-80861	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: bail out of setup if the controller is inaccessible xhci_gen_setup() locates the operational registers using the capability length read from the very first register: xhci->op_regs = hcd->regs + HC_LENGTH(readl(&xhci->cap_regs->hc_capbase)); If the controller is dead or has dropped off the bus, that read returns ~0, HC_LENGTH() truncates it to 0xff, and op_regs ends up 0xff bytes past the page-aligned MMIO base, i.e. unaligned. The first access through it, xhci_halt() -> xhci_handshake() reading op_regs->status, is then an unaligned readl() on device memory. arm64 faults on unaligned device accesses, so instead of xhci_handshake() catching the all-ones value and returning -ENODEV, setup oopses: xhci-pci-renesas 0005:08:00.0: Unable to change power state from D3cold to D0, device inaccessible xhci-pci-renesas 0005:08:00.0: xHCI Host Controller xhci-pci-renesas 0005:08:00.0: new USB bus registered, assigned bus number 1 Unable to handle kernel paging request at virtual address ffff80030a770103 ESR = 0x0000000096000021 FSC = 0x21: alignment fault Internal error: Oops: 0000000096000021 [#1] SMP pc : xhci_halt [xhci_hcd] Call trace: xhci_halt xhci_gen_setup xhci_pci_setup usb_add_hcd usb_hcd_pci_probe xhci_pci_common_probe xhci_pci_renesas_probe This was hit with a Renesas uPD720201 that failed to power up ("Unable to change power state from D3cold to D0, device inaccessible") yet still reached the HCD probe path. Read the capability register once, and if it reads back the all-ones value (as xhci_handshake() and xhci_reset() already test for), abort setup with -ENODEV before op_regs is derived from it. Reading it once also avoids re-reading a register that may change under a concurrent hot-removal.	N/A	More Details
CVE-2026-80862	In the Linux kernel, the following vulnerability has been resolved: nvme-tcp: fix usage of page_frag_cache nvme uses page_frag_cache to preallocate PDU for each preallocated request of block device. Block devices are created in parallel threads, consequently page_frag_cache is used in not thread-safe manner. That leads to incorrect refcounting of backstore pages and premature free. That can be catched by !sendpage_ok inside network stack: WARNING: CPU: 7 PID: 467 at ../net/core/skbuff.c:6931 skb_splice_from_iter+0xfa/0x310. tcp_sendmsg_locked+0x782/0xce0 tcp_sendmsg+0x27/0x40 sock_sendmsg+0x8b/0xa0 nvme_tcp_try_send_cmd_pdu+0x149/0x2a0 Then random panic may occur. Fix that by serializing the usage of page_frag_cache.	N/A	More Details
CVE-2026-80863	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix OOB in free_rd_atomic_resources() free_rd_atomic_resources() iterates using qp->attr.max_dest_rd_atomic. Updating max_dest_rd_atomic before freeing the old array can make the free path walk past the old allocation and trigger a slab out-of-bounds write catched by KASAN: == BUG: KASAN: slab-out-of-bounds in free_rd_atomic_resource drivers/infiniband/sw/rxe/rxe_qp.c:180 [inline] BUG: KASAN: slab-out-of-bounds in free_rd_atomic_resources drivers/infiniband/sw/rxe/rxe_qp.c:171 [inline] BUG: KASAN: slab-out-of-bounds in free_rd_atomic_resources drivers/infiniband/sw/rxe/rxe_qp.c:163 [inline] BUG: KASAN: slab-out-of-bounds in rxe_qp_from_attr+0x1e88/0x2150 drivers/infiniband/sw/rxe/rxe_qp.c:712 Write of size 4 at addr ffff88802b8dddb8 by task syz.3.451/11063 CPU: 0 UID: 0 PID: 11063 Comm: syz.3.451 Not tainted 7.1.0 #2 PREEMPT(full) Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x10e/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xf7/0x600 mm/kasan/report.c:482 kasan_report+0xe4/0x120 mm/kasan/report.c:595 free_rd_atomic_resource drivers/infiniband/sw/rxe/rxe_qp.c:180 [inline] free_rd_atomic_resources drivers/infiniband/sw/rxe/rxe_qp.c:171 [inline] free_rd_atomic_resources drivers/infiniband/sw/rxe/rxe_qp.c:163 [inline] rxe_qp_from_attr+0x1e88/0x2150 drivers/infiniband/sw/rxe/rxe_qp.c:712 rxe_modify_qp+0x1e2/0x530 drivers/infiniband/sw/rxe/rxe_verbs.c:623 ib_security_modify_qp+0x223/0xfa0 drivers/infiniband/core/security.c:625 _ib_modify_qp+0x333/0xec0 drivers/infiniband/core/verbs.c:1915 modify_qp+0x13ca/0x1940 drivers/infiniband/core/uverbs_cmd.c:1932 ib_uverbs_modify_qp+0xcb/0x120 drivers/infiniband/core/uverbs_cmd.c:1958 ib_uverbs_write+0xb86/0x1030 drivers/infiniband/core/uverbs_main.c:680 vfs_write+0x2aa/0x1070 fs/read_write.c:686 ksys_write+0x1f8/0x250 fs/read_write.c:740 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x116/0x800 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fefc75a70cd Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 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 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fefc8495018 EFLAGS: 00000246 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00007fefc7835fa0 RCX: 00007fefc75a70cd RDX: 0000000000000078 RSI: 0000200000000240 RDI: 0000000000000007 RBP: 00007fefc764f10f R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fefc7836038 R14:	N/A	More Details

	00007fefc7835fa0 R15: 00007ffcf0586aa0 </TASK> Allocated by task 11063: kasan_save_stack+0x33/0x60 mm/kasan/common.c:57 kasan_save_track+0x14/0x30 mm/kasan/common.c:78 poison_kmalloc_redzone mm/kasan/common.c:398 [inline] __kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:415 kasan_kmalloc include/linux/kasan.h:263 [inline] __do_kmalloc_node mm/slub.c:5296 [inline] __kmalloc_noprof+0x32a/0x850 mm/slub.c:5308 kmalloc_noprof include/linux/slab.h:954 [inline] kzalloc_noprof include/linux/slab.h:1188 [inline] alloc_rd_atomic_resources drivers/infiniband/sw/rxe/rxe_qp.c:155 [inline] rxe_qp_from_attr+0x3f8/0x2150 drivers/infiniband/sw/rxe/rxe_qp.c:714 rxe_modify_qp+0x1e2/0x530 drivers/infiniband/sw/rxe/rxe_verbs.c:623 ib_security_modify_qp+0x223/0xfa0 drivers/infiniband/core/security.c:625 _ib_modify_qp+0x333/0xec0 drivers/infiniband/core/verbs.c:1915 modify_qp+0x13ca/0x1940 drivers/infiniband/core/uverbs_cmd.c:1932 ib_uverbs_modify_qp+0xcb/0x120 drivers/infiniband/core/uverbs_cmd.c:1958 ib_uverbs_write+0xb86/0x1030 drivers/infiniband/core/uverbs_ma ---truncated---		
CVE-2026-80864	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix responder UAF on IB_QP_MAX_DEST_RD_ATOMIC modify_qp rxe_qp_from_attr() handles IB_QP_MAX_DEST_RD_ATOMIC outside the IB_QP_STATE path, so it holds no state_lock and runs while the responder task rxe_receiver() (recv_task on rxe_wq) is live. A modify_qp() setting only that attribute calls free_rd_atomic_resources() then alloc_rd_atomic_resources(), swapping qp->resp.resources[] while rxe_prepare_res()/find_resource() walk it; free_rd_atomic_resources() also leaves the cached pointer qp->resp.res dangling. A local unprivileged user can race the free/realloc into a use-after-free in rxe_receiver() (local DoS). Drain recv_task around the swap with rxe_disable_task()/rxe_enable_task(), as rxe_qp_reset() already does when tearing this array down, re-enabling only after alloc_rd_atomic_resources() succeeds so the responder never resumes against a NULL qp->resp.resources on the ENOMEM path. Also clear qp->resp.res in free_rd_atomic_resources(), like the rxe_resp.c completion paths. Reproduced under KASAN; the slab-use-after-free in rxe_receiver() is gone.	N/A	More Details
CVE-2026-82911	Cross-Site Request Forgery (CSRF) in the OrderConfirmController at GET /order/confirm/{order_number} in Roskus Prospero Flow CRM before 5.15.11 allows an unauthenticated attacker to confirm any order on behalf of an authenticated user by directing them to a crafted page. Laravel's VerifyCsrfToken middleware enforces CSRF tokens only on POST, PUT, PATCH, and DELETE requests; the Route::get declaration leaves this state-changing action unprotected. Session cookies configured with SameSite=Lax are automatically included in top-level cross-site navigation, so a single link click triggers OrderConfirmController::confirm() and transitions the target order from pending to confirmed without user authorization. Because order numbers are sequential integers, an attacker can enumerate and confirm all existing orders in a single automated sweep.	N/A	More Details
CVE-2026-38961	Cross-Site Scripting (XSS) vulnerability in the RSS Widget of Netgate pfSense Plus (versions 26.03, 25.11.1) and pfSense CE (version 2.8.1) allows remote authenticated attackers to inject arbitrary JavaScript via malicious content in an RSS feed title. The injected script executes in the browser of any authenticated user who views the dashboard, due to insufficient sanitization of feed title data before rendering in the widget.	N/A	More Details
CVE-2026-80872	In the Linux kernel, the following vulnerability has been resolved: ALSA: hda/tas2781: Cancel async firmware request at unbind TAS2781 HDA I2C and SPI queue RCA firmware loading from component bind with request_firmware_nowait(). The firmware loader keeps the callback module pinned and holds a device reference, but the callback still uses driver-private HDA state. Component unbind removes controls and DSP state immediately. Later device removal tears down the TAS2781 private data, including codec_lock. If the async firmware callback runs after unbind has started, it can operate on state that is being torn down. Cancel or synchronize the async firmware request before removing controls and DSP state. A queued callback is cancelled, and an already-running callback is allowed to finish before unbind continues.	N/A	More Details
CVE-2026-78849	Cross Site Scripting vulnerability in Netgate pfSense Plus software versions <= 26.03 pfSense CE software versions <= 2.8.1 allows a remote attacker to execute arbitrary code via the captive_portal_status.widget.php file	N/A	More Details
CVE-2026-80865	In the Linux kernel, the following vulnerability has been resolved: bpf: Add missing access_ok call to copy_user_syms As reported by sashiko we use __get_user without prior access_ok call on the user space pointer. Adding the missing call for the whole pointer array. Plus removing the err check in the error path, because it's not needed and also we can return -ENOMEM directly from the first kvmalloc_array fail path. [1] https://lore.kernel.org/bpf/20260611115503.AC16D1F00893@smtp.kernel.org/	N/A	More Details
CVE-2026-80866	In the Linux kernel, the following vulnerability has been resolved: tipc: avoid busy looping in tipc_exit_net() Blamed commit introduced a busy-wait loop in tipc_exit_net() to wait for pending UDP bearer cleanup works to complete: while (atomic_read(&tn->wq_count)) cond_resched(); This loop can busy-wait for a long time if cond_resched() is a NOP. This typically happens if the netns exit is executed by a high priority task, or under kernels configured without preemption (CONFIG_PREEMPT_NONE). In such cases, it wastes CPU cycles and can lead to soft lockups. Fix this by replacing the busy loop with wait_var_event(), allowing the thread to sleep properly until the work queue count reaches zero. Accordingly, update cleanup_bearer() to use atomic_dec_and_test() and wake_up_var() to wake up the waiter when the count drops to zero. This uses the global wait queue hash table, avoiding the need to bloat struct tipc_net with a wait_queue_head_t. The atomic_dec_and_test() provides the necessary memory barrier to ensure the wakeup is not missed.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: alpha/PCI: Add security_locked_down() check to pci_mmap_resource() Currently, Alpha's pci_mmap_resource() does not check		

2026-80867	security_locked_down(LOCKDOWN_PCI_ACCESS) before allowing userspace to mmap PCI BARs. The generic version has had this check since commit eb627e17727e ("PCI: Lock down BAR access when the kernel is locked down") to prevent DMA attacks when the kernel is locked down. Add the same check to Alpha's pci_mmap_resource().	N/A	More Details
CVE-2026-80868	In the Linux kernel, the following vulnerability has been resolved: ntfs3: Allocate iomap inline_data using alloc_page This fixes a BUG reported in iomap_write_end_inline: iomap_inline_data_valid checks that the inline_data fits within a page. If the inline_data is allocated with kmemdup there's no guarantee that it's page-aligned, so the check sometimes fails. Allocate it with alloc_page to ensure it's page-aligned.	N/A	More Details
CVE-2026-80869	In the Linux kernel, the following vulnerability has been resolved: ntfs: bound the attribute-list entry in ntfs_read_inode_mount() The $MFT attribute-list walk in ntfs_read_inode_mount() validates each entry only with "(u8 *)al_entry + 6 > al_end" and "(u8 *)al_entry + le16_to_cpu(al_entry->length) > al_end", but then reads al_entry->lowest_vcn (an __le64 at offset 8) and al_entry->mft_reference (offset 16) -- fields beyond the 6 bytes proven in range. al_entry->length is attacker-controlled and only required non-zero, so a short entry (e.g. length 8) placed at the tail passes both checks while the lowest_vcn / mft_reference reads fall past al_end. al_end is ni->attr_list + attr_list_size (the on-disk size); the buffer is kvzalloc(round_up(attr_list_size, SECTOR_SIZE)), so the sector rounding usually absorbs the over-read -- but when attr_list_size is a multiple of SECTOR_SIZE there is no slack and a crafted $MFT attribute list produces an out-of-bounds read at mount time. Validate the entry with ntfs_attr_list_entry_is_valid() (added in patch 1/3) before dereferencing it, matching the bound the other attribute-list walks now use. The validator already requires the length to cover the fixed header, which makes the separate "!al_entry->length" check redundant, so drop it too.	N/A	More Details
CVE-2026-80870	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Validate CRIU-restored IDs before idr_alloc The KFD CRIU restore flow restores previously saved object IDs from userspace. For event restore: kfd_criu_restore_event() -> create_signal_event() / create_other_event() -> allocate_event_notification_slot() -> idr_alloc(..., *restore_id, *restore_id + 1, ...) For BO restore: criu_restore_memory_of_gpu() -> idr_alloc(..., bo_priv->idr_handle, ...) In both cases, the restored ID comes from userspace-provided CRIU data. idr_alloc() expects the ID range values to fit within signed int limits. If a restored ID is larger than INT_MAX, it can trigger a WARN in the IDR layer. A kernel WARN is undesirable because it prints a warning trace and may cause a panic or reboot on systems with panic_on_warn enabled. Smatch reported these paths as allowing unchecked userspace values to reach idr_alloc(). Add INT_MAX validation before using restored IDs in: - kfd_criu_restore_event() - criu_restore_memory_of_gpu() If the restored ID is invalid, return -EINVAL. This prevents invalid restore data from reaching the IDR layer and avoids WARN-triggering paths, while keeping valid restore behavior unchanged.	N/A	More Details
CVE-2026-80871	In the Linux kernel, the following vulnerability has been resolved: crypto: xilinx-trng - Remove crypto_rng interface Implementing the crypto_rng interface has no purpose, as it isn't used in practice. It's being removed from other drivers too. Just remove it. This leaves hwrng, which is actually used. Tagging with 'Cc stable' due to the bugs that this removes: - xtrng_trng_generate() sometimes returned success even when it didn't fill in all the bytes. - It was possible for xtrng_trng_generate() and xtrng_hwrng_trng_read() to run concurrently and interfere with each other, as the locking code in xtrng_hwrng_trng_read() was broken.	N/A	More Details
CVE-2026-80805	In the Linux kernel, the following vulnerability has been resolved: xfs: validate attr entry pointer before field access xfs_attr3_leaf_verify_entry() accesses lentry/rentry fields (namelen, valuelen) before checking if the entry pointer itself is within bounds. If nameidx is crafted to point near the end of the buffer, these field accesses can read out-of-bounds before the bounds check at name_end > buf_end is performed. Add explicit bounds checks for entry pointers before accessing their fields. Use offsetof() to check that the start of the flexible array member (nameval/name) is within bounds, which ensures all preceding fields are safe to access.	N/A	More Details