SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 April 2026

Generated on 15 April 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-2026-40175	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0 and 0.3.1, the Axios library is vulnerable to a specific "Gadget" attack chain that allows Prototype Pollution in any third-party dependency to be escalated into Remote Code Execution (RCE) or Full Cloud Compromise (via AWS IMDSv2 bypass). This vulnerability is fixed in 1.15.0 and 0.3.1.	10.0	More Details
CVE-2026-40089	Sonicverse is a Self-hosted Docker Compose stack for live radio streaming. The Sonicverse Radio Audio Streaming Stack dashboard contains a Server-Side Request Forgery (SSRF) vulnerability in its API client (apps/dashboard/lib/api.ts). Installations created using the provided install.sh script (including the one-liner bash <(curl -fsSL https://sonicverse.short.gy/install-audiostack)) are affected. In these deployments, the dashboard accepts user-controlled URLs and passes them directly to a server-side HTTP client without sufficient validation. An authenticated operator can abuse this to make arbitrary HTTP requests from the dashboard backend to internal or external systems. This vulnerability is fixed with commit cb1ddbacafcb441549fe87d3eeabdb6a085325e4.	9.9	More Details
CVE-2026-27681	Due to insufficient authorization checks in SAP Business Planning and Consolidation and SAP Business Warehouse, an authenticated user can execute crafted SQL statements to read, modify, and delete database data. This leads to a high impact on the confidentiality, integrity, and availability of the system.	9.9	More Details
CVE-2025-62718	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0 and 0.31.0, Axios does not correctly handle hostname normalization when checking NO_PROXY rules. Requests to loopback addresses like localhost. (with a trailing dot) or [::1] (IPv6 literal) skip NO_PROXY matching and go through the configured proxy. This goes against what developers expect and lets attackers force requests through a proxy, even if NO_PROXY is set up to protect loopback or internal services. This issue leads to the possibility of proxy bypass and SSRF vulnerabilities allowing attackers to reach sensitive loopback or internal services despite the configured protections. This vulnerability is fixed in 1.15.0 and 0.31.0.	9.9	More Details
CVE-2026-39888	PraisonAI is a multi-agent teams system. Prior to 1.5.115, execute_code() in praisonaiagents.tools.python_tools defaults to sandbox_mode="sandbox", which runs user code in a subprocess wrapped with a restricted __builtins__ dict and an AST-based blocklist. The AST blocklist embedded inside the subprocess wrapper (blocked_attrs of python_tools.py) contains only 11 attribute names — a strict subset of the 30+ names blocked in the direct-execution path. The four attributes that form a frame-traversal chain out of the sandbox are all absent from the subprocess list (__traceback__, tb_frame, f_back, and f_builtins). Chaining these attributes through a caught exception exposes the real Python builtins dict of the subprocess wrapper frame, from which exec can be retrieved and called under a non-blocked variable name — bypassing every remaining security layer. This vulnerability is fixed in 1.5.115.	9.9	More Details
CVE-2026-38526	An authenticated arbitrary file upload vulnerability in the /admin/tinymce/upload endpoint of Webkul Krayin CRM v2.2.x allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.9	More Details
	In Juju versions prior to 2.9.57 and 3.6.21, an authorization issue exists in the Controller facade. An		

CVE-2026-5412	authenticated user can call the CloudSpec API method to extract the cloud credentials used to bootstrap the controller. This allows a low-privileged user to access sensitive credentials. This issue is resolved in Juju versions 2.9.57 and 3.6.21.	9.9	More Details
CVE-2026-35031	Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chain in the subtitle upload endpoint (POST /Videos/{itemId}/Subtitles), where the Format field is not validated, allowing path traversal via the file extension and enabling arbitrary file write. This arbitrary file write can be chained into arbitrary file read via .strm files, database extraction, admin privilege escalation, and ultimately remote code execution as root via ld.so.preload. Exploitation requires an administrator account or a user that has been explicitly granted the "Upload Subtitles" permission. This issue has been fixed in version 10.11.7. If users are unable to upgrade immediately, they can grant non-administrator users Subtitle upload permissions to reduce attack surface.	9.9	More Details
CVE-2026-5978	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected is the function setWiFiAclRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument mode leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-6029	A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setVpnAccountCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument User results in os command injection. The attack may be launched remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2026-6028	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Impacted is the function setPptpServerCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument enable leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-5976	A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setStorageCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument sambaEnabled results in os command injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-6027	A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. This issue affects the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument enable can lead to os command injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-6026	A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This vulnerability affects the function setPortalConfWeChat of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument enable results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-6025	A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument enable leads to os command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-5977	A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. This impacts the function setWiFiBasicCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument wifiOff can lead to os command injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-33784	A Use of Default Password vulnerability in the Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows an unauthenticated, network-based attacker to take full control of the device. vLWC software images ship with an initial password for a high privileged account. A change of this password is not enforced during the provisioning of the software, which can make full access to the system by unauthorized actors possible.This issue affects all versions of vLWC before 3.0.94.	9.8	More Details
CVE-2026-6154	A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setWizardCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument wizard results in os command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-5996	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. The affected element is the function setAdvancedInfoShow of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument tty_server leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-5995	A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. Impacted is the function setMiniuiHomeInfoShow of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument lan_info can lead to os command injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-27143	Arithmetic over induction variables in loops were not correctly checked for underflow or overflow. As a result, the compiler would allow for invalid indexing to occur at runtime, potentially leading to memory corruption.	9.8	More Details

CVE-2026-5994	A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This issue affects the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument telnet_enabled results in os command injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-5993	A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. This vulnerability affects the function setWiFiGuestCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument wifiOff leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-34424	Smart Slider 3 Pro version 3.5.1.35 for WordPress and Joomla contains a multi-stage remote access toolkit injected through a compromised update system that allows unauthenticated attackers to execute arbitrary code and commands. Attackers can trigger pre-authentication remote shell execution via HTTP headers, establish authenticated backdoors accepting arbitrary PHP code or OS commands, create hidden administrator accounts, exfiltrate credentials and access keys, and maintain persistence through multiple injection points including must-use plugins and core file modifications.	9.8	More Details
CVE-2026-5997	A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the function setLoginPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument admpass results in os command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2026-6057	FalkorDB Browser 1.9.3 contains an unauthenticated path traversal vulnerability in the file upload API that allows remote attackers to write arbitrary files and achieve remote code execution.	9.8	More Details
CVE-2025-44560	owntone-server 2ca10d9 is vulnerable to Buffer Overflow due to lack of recursive checking.	9.8	More Details
CVE-2026-6138	A flaw has been found in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the function setAccessDeviceCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument mac causes os command injection. The attack can be initiated remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2026-6116	A vulnerability has been found in Totolink A7100RU 7.4cu.2313_b20191024. This vulnerability affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument ip leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2026-6115	A flaw has been found in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setAppCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument enable can lead to os command injection. The attack may be launched remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2026-6114	A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setNetworkCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument proto results in os command injection. The attack may be initiated remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2026-6113	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this vulnerability is the function setTtyServiceCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument ttyEnable leads to os command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-6112	A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. Affected is the function setRadvdCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument maxRtrAdvInterval causes os command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-6132	A vulnerability was determined in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setLedCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument enable causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	9.8	More Details
CVE-2026-40189	goshs is a SimpleHTTPServer written in Go. Prior to 2.0.0-beta.4, goshs enforces the documented per-folder .goshs ACL/basic-auth mechanism for directory listings and file reads, but it does not enforce the same authorization checks for state-changing routes. An unauthenticated attacker can upload files with PUT, upload files with multipart POST /upload, create directories with ?mkdir, and delete files with ?delete inside a .goshs-protected directory. By deleting the .goshs file itself, the attacker can remove the folder's auth policy and then access previously protected content without credentials. This results in a critical authorization bypass affecting confidentiality, integrity, and availability. This vulnerability is fixed in 2.0.0-beta.4.	9.8	More Details
CVE-2026-6139	A vulnerability has been found in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function UploadOpenVpnCert of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument FileName leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	9.8	More Details
	A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the		

CVE-2026-5975	function setDmzCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument wanIdx leads to os command injection. The attack may be performed from remote. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-6140	A vulnerability was found in Totolink A7100RU 7.4cu.2313_b20191024. This impacts the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument FileName results in os command injection. The attack may be initiated remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-23781	An issue was discovered in BMC Control-M/MFT 9.0.20 through 9.0.22. A set of default debug user credentials is hardcoded in cleartext within the application package. If left unchanged, these credentials can be easily obtained and may allow unauthorized access to the MFT API debug interface.	9.8	More Details
CVE-2026-36236	SourceCodester Engineers Online Portal v1.0 is vulnerable to SQL Injection in update_password.php via the new_password parameter.	9.8	More Details
CVE-2026-36235	A SQL injection vulnerability was found in the scheduleSubList.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that the 'subjcode' parameter is directly embedded into the SQL query via string interpolation without any sanitization or validation.	9.8	More Details
CVE-2026-36234	itsourcecode Online Student Enrollment System v1.0 is vulnerable to SQL Injection in newCourse.php via the 'coursename' parameter.	9.8	More Details
CVE-2026-36233	A SQL injection vulnerability was found in the assignInstructorSubjects.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that attackers can inject malicious code via the parameter "subjcode" and use it directly in SQL queries without the need for appropriate cleaning or validation.	9.8	More Details
CVE-2026-36232	A SQL injection vulnerability was found in the instructorClasses.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that the 'classId' parameter from $_GET['classId'] is directly concatenated into the SQL query without any sanitization or validation.	9.8	More Details
CVE-2026-29861	PHP-MYSQL-User-Login-System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter at login.php.	9.8	More Details
CVE-2026-6156	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setIpQosRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument Comment leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-6155	A weakness has been identified in Totolink A7100RU 7.4cu.2313. The impacted element is the function setWanCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument pppoeServiceName can lead to os command injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-6131	A vulnerability was found in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this vulnerability is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument command results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2026-5902	Race in Media in Google Chrome on Android prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to corrupt media stream metadata via a crafted HTML page. (Chromium security severity: Low)	9.8	More Details
CVE-2026-40288	PraisonAI is a multi-agent teams system. In versions below 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents, the workflow engine is vulnerable to arbitrary command and code execution through untrusted YAML files. When praisonai workflow run <file.yaml> loads a YAML file with type: job, the JobWorkflowExecutor in job_workflow.py processes steps that support run: (shell commands via subprocess.run()), script: (inline Python via exec()), and python: (arbitrary Python script execution)—all without any validation, sandboxing, or user confirmation. The affected code paths include action_run() in workflow.py and _exec_shell(), _exec_inline_python(), and _exec_python_script() in job_workflow.py. An attacker who can supply or influence a workflow YAML file (particularly in CI pipelines, shared repositories, or multi-tenant deployment environments) can achieve full arbitrary command execution on the host system, compromising the machine and any accessible data or credentials. This issue has been fixed in versions 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents.	9.8	More Details
CVE-2025-63939	Improper input handling in /Grocery/search_products_itname.php, in anirudhkannan Grocery Store Management System 1.0, allows SQL injection via the sitem_name POST parameter.	9.8	More Details
CVE-2026-39890	PraisonAI is a multi-agent teams system. Prior to 4.5.115, the AgentService.loadAgentFromFile method uses the js-yaml library to parse YAML files without disabling dangerous tags (such as !!js/function and !!js/undefined). This allows an attacker to craft a malicious YAML file that, when parsed, executes arbitrary JavaScript code. An attacker can exploit this vulnerability by uploading a malicious agent definition file via the API endpoint, leading to remote code execution (RCE) on the server. This vulnerability is fixed in 4.5.115.	9.8	More Details
CVE-2025-65135	In manikandan580 School-management-system 1.0, a time-based blind SQL injection vulnerability exists in /studentms/admin/between-date-reprtsdetails.php through the fromdate POST parameter.	9.8	More Details
	The ProSolution WP Client plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type		

CVE-2026-2942	validation in the 'proSol_fileUploadProcess' function in all versions up to, and including, 1.9.9. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-52221	Tenda AC6 15.03.05.16_multi is vulnerable to Buffer Overflow in the formSetCfm function via the funcname, funcpara1, and funcpara2 parameters.	9.8	More Details
CVE-2026-39808	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSandbox 4.4.0 through 4.4.8 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	9.8	More Details
CVE-2026-33229	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Prior to 17.4.8 and 17.10.1, an improperly protected scripting API allows any user with script right to bypass the sandboxing of the Velocity scripting API and execute, e.g., arbitrary Python scripts, allowing full access to the XWiki instance and thereby compromising the confidentiality, integrity and availability of the whole instance. Note that script right already constitutes a high level of access that we don't recommend giving to untrusted users. This vulnerability is fixed in 17.4.8 and 17.10.1.	9.8	More Details
CVE-2026-31040	A vulnerability was identified in stata-mcp prior to v1.13.0 where insufficient validation of user-supplied Stata do-file content can lead to command execution.	9.8	More Details
CVE-2026-39813	A path traversal: '../filedir' vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8 may allow attacker to escalation of privilege via <insert attack vector here>	9.8	More Details
CVE-2026-33824	Double free in Windows IKE Extension allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-3535	The DSGVO Google Web Fonts GDPR plugin for WordPress is vulnerable to arbitrary file upload due to missing file type validation in the `DSGVOGWPdownloadGoogleFonts()` function in all versions up to, and including, 1.1. The function is exposed via a `wp_ajax_nopriv_` hook, requiring no authentication. It fetches a user-supplied URL as a CSS file, extracts URLs from its content, and downloads those files to a publicly accessible directory without validating the file type. This makes it possible for unauthenticated attackers to upload arbitrary files including PHP webshells, leading to remote code execution. The exploit requires the site to use one of a handful of specific themes (twentyfifteen, twentyseventeen, twentysixteen, storefront, salient, or shapely).	9.8	More Details
CVE-2026-4003	The Users manager – PN plugin for WordPress is vulnerable to Privilege Escalation via Arbitrary User Meta Update in all versions up to and including 1.1.15. This is due to a flawed authorization logic check in the userspn_ajax_nopriv_server() function within the 'userspn_form_save' case. The conditional only blocks unauthenticated users when the user_id is empty, but when a non-empty user_id is supplied, execution bypasses this check entirely and proceeds to update arbitrary user meta via update_user_meta() without any authentication or authorization verification. Additionally, the nonce required for this AJAX endpoint ('userspn-nonce') is exposed to all visitors via wp_localize_script on the public wp_enqueue_scripts hook, rendering the nonce check ineffective as a security control. This makes it possible for unauthenticated attackers to update arbitrary user metadata for any user account, including the userspn_secret_token field.	9.8	More Details
CVE-2026-3296	The Everest Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.4.3 via deserialization of untrusted input from form entry metadata. This is due to the html-admin-page-entries-view.php file calling PHP's native unserialize() on stored entry meta values without passing the allowed_classes parameter. This makes it possible for unauthenticated attackers to inject a serialized PHP object payload through any public Everest Forms form field. The payload survives sanitize_text_field() sanitization (serialization control characters are not stripped) and is stored in the wp_evf_entrymeta database table. When an administrator views entries or views an individual entry, the unsafe unserialize() call processes the stored data without class restrictions.	9.8	More Details
CVE-2026-1830	The Quick Playground plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.3.1. This is due to insufficient authorization checks on REST API endpoints that expose a sync code and allow arbitrary file uploads. This makes it possible for unauthenticated attackers to retrieve the sync code, upload PHP files with path traversal, and achieve remote code execution on the server.	9.8	More Details
CVE-2026-5850	A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setVpnPassCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument pptpPassThru leads to os command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	9.8	More Details
CVE-2026-5851	A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This impacts the function setUPnPCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument enable results in os command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	9.8	More Details
CVE-2026-5852	A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. Affected is the function setIptvCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument igmpVer causes os command injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2025-13926	An attacker could use data obtained by sniffing the network traffic to forge packets in order to make arbitrary requests to Contemporary Controls BASC 20T.	9.8	More Details

CVE-2026-31282	Totara LMS v19.1.5 and before is vulnerable to Incorrect Access Control. The login page code can be manipulated to reveal the login form. An attacker can chain that with missing rate-limit on the login form to launch a brute force attack.	9.8	More Details
CVE-2026-31170	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stun-pass parameter to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-31283	In Totara LMS v19.1.5 and before, the forgot password API does not implement rate limiting for the target email address. which can be used for an Email Bombing attack.	9.8	More Details
CVE-2026-6195	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument admpass leads to os command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2026-40042	Pachno 1.0.6 contains an XML external entity injection vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting unsafe XML parsing in the TextParser helper. Attackers can inject malicious XML entities through wiki table syntax and inline tags in issue descriptions, comments, and wiki articles to trigger entity resolution via simplexml_load_string() without LIBXML_NONET restrictions.	9.8	More Details
CVE-2026-40044	Pachno 1.0.6 contains a deserialization vulnerability that allows unauthenticated attackers to execute arbitrary code by injecting malicious serialized objects into cache files. Attackers can write PHP object payloads to world-writable cache files with predictable names in the cache directory, which are unserialized during framework bootstrap before authentication checks occur.	9.8	More Details
CVE-2026-5443	A heap buffer overflow vulnerability exists during the decoding of `PALETTE COLOR` DICOM images. Pixel length validation uses 32-bit multiplication for width and height calculations. If these values overflow, the validation check incorrectly succeeds, allowing the decoder to read and write to memory beyond allocated buffers.	9.8	More Details
CVE-2026-5442	A heap buffer overflow vulnerability exists in the DICOM image decoder. Dimension fields are encoded using Value Representation (VR) Unsigned Long (UL), instead of the expected VR Unsigned Short (US), which allows extremely large dimensions to be processed. This causes an integer overflow during frame size calculation and results in out-of-bounds memory access during image decoding.	9.8	More Details
CVE-2026-22562	A malicious actor with access to the UniFi Play network could exploit a Path Traversal vulnerability found in the device firmware to write files on the system that could be used for a remote code execution (RCE). Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier)UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or laterUpdate UniFi Play Audio Port to Version 1.1.9 or later	9.8	More Details
CVE-2026-22563	A series of Improper Input Validation vulnerabilities could allow a Command Injection by a malicious actor with access to the UniFi Play network. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later	9.8	More Details
CVE-2026-22564	An Improper Access Control vulnerability could allow a malicious actor with access to the UniFi Play network to enable SSH to make unauthorized changes to the system. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later	9.8	More Details
CVE-2026-6264	A critical vulnerability in the Talend JobServer and Talend Runtime allows unauthenticated remote code execution via the JMX monitoring port. The attack vector is the JMX monitoring port of the Talend JobServer. The vulnerability can be mitigated for the Talend JobServer by requiring TLS client authentication for the monitoring port; however, the patch must be applied for full mitigation. For Talend ESB Runtime, the vulnerability can be mitigated by disabling the JobServer JMX monitoring port, which is disabled by default from the R2024-07-RT patch.	9.8	More Details
CVE-2026-5854	A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setWiFiEasyCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument merge results in os command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	9.8	More Details
CVE-2026-5853	A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this vulnerability is the function setIpv6LanCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument addrPrefixLen leads to os command injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	9.8	More Details
CVE-2019-25709	CF Image Hosting Script 1.6.5 allows unauthenticated attackers to download and decode the application database by accessing the imgdb.db file in the upload/data directory. Attackers can extract delete IDs stored in plaintext from the deserialized database and use them to delete all pictures via the d parameter.	9.8	More Details
CVE-2026-27303	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	9.6	More Details
	NuGet Gallery is a package repository that powers nuget.org. A security vulnerability exists in the NuGetGallery		

CVE-2026-39399	backend job’s handling of .nuspec files within NuGet packages. An attacker can supply a crafted nuspec file with malicious metadata, leading to cross package metadata injection that may result in remote code execution (RCE) and/or arbitrary blob writes due to insufficient input validation. The issue is exploitable via URI fragment injection using unsanitized package identifiers, allowing an attacker to control the resolved blob path. This enables writes to arbitrary blobs within the storage container, not limited to .nupkg files, resulting in potential tampering of existing content. This issue has been patched in commit 0e80f87628349207cdcaf55358491f8a6f1ca276.	9.6	More Details
CVE-2026-5874	Use after free in PrivateAI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	9.6	More Details
CVE-2026-30232	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 4.8.5, Chartbrew allows authenticated users to create API data connections with arbitrary URLs. The server fetches these URLs using request-promise without any IP address validation, enabling Server-Side Request Forgery attacks against internal networks and cloud metadata endpoints. This vulnerability is fixed in 4.8.5.	9.6	More Details
CVE-2026-39617	Cross-Site Request Forgery (CSRF) vulnerability in priyanshumittal Bluestreet bluestreet allows Cross Site Request Forgery.This issue affects Bluestreet: from n/a through <= 1.7.3.	9.6	More Details
CVE-2026-40088	PraisonAI is a multi-agent teams system. Prior to 4.5.121, the execute_command function and workflow shell execution are exposed to user-controlled input via agent workflows, YAML definitions, and LLM-generated tool calls, allowing attackers to inject arbitrary shell commands through shell metacharacters. This vulnerability is fixed in 4.5.121.	9.6	More Details
CVE-2026-39619	Cross-Site Request Forgery (CSRF) vulnerability in priyanshumittal Busiprof busiprof allows Upload a Web Shell to a Web Server.This issue affects Busiprof: from n/a through <= 2.5.2.	9.6	More Details
CVE-2026-39620	Cross-Site Request Forgery (CSRF) vulnerability in priyanshumittal Appointment appointment allows Upload a Web Shell to a Web Server.This issue affects Appointment: from n/a through <= 3.5.5.	9.6	More Details
CVE-2026-39640	Cross-Site Request Forgery (CSRF) vulnerability in mndpsingh287 Theme Editor theme-editor allows Code Injection.This issue affects Theme Editor: from n/a through <= 3.2.	9.6	More Details
CVE-2026-33707	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, the default password reset mechanism generates tokens using sha1($email) with no random component, no expiration, and no rate limiting. An attacker who knows a user's email can compute the reset token and change the victim's password without authentication. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	9.4	More Details
CVE-2026-27304	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	9.3	More Details
CVE-2026-5752	Sandbox Escape Vulnerability in Terrarium allows arbitrary code execution with root privileges on a host process via JavaScript prototype chain traversal.	9.3	More Details
CVE-2026-34615	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	9.3	More Details
CVE-2026-27246	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	9.3	More Details
CVE-2026-27245	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed.	9.3	More Details
CVE-2026-27243	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed.	9.3	More Details
CVE-2026-31845	A reflected cross-site scripting (XSS) vulnerability exists in Rukovoditel CRM version 3.6.4 and earlier in the Zadarma telephony API endpoint (/api/tel/zadarma.php). The application directly reflects user-supplied input from the 'zd_echo' GET parameter into the HTTP response without proper sanitization, output encoding, or content-type restrictions. The vulnerable code is: if (isset($_GET['zd_echo'])) exit($_GET['zd_echo']); An unauthenticated attacker can exploit this issue by crafting a malicious URL containing JavaScript payloads. When a victim visits the link, the payload executes in the context of the application within the victim's browser, potentially leading to session hijacking, credential theft, phishing, or account takeover. The issue is fixed in version 3.7, which introduces proper input validation and output encoding to prevent script injection.	9.3	More Details
CVE-2026-1346	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated user to escalate their privileges to root due to execution	9.3	More Details

	with unnecessary privileges than required.		
CVE-2026-40154	PraisonAI is a multi-agent teams system. Prior to 4.5.128, PraisonAI treats remotely fetched template files as trusted executable code without integrity verification, origin validation, or user confirmation, enabling supply chain attacks through malicious templates. This vulnerability is fixed in 4.5.128.	9.3	More Details
CVE-2026-34178	In Canonical LXD before 6.8, the backup import path validates project restrictions against backup/index.yaml in the supplied tar archive but creates the instance from backup/container/backup.yaml, a separate file in the same archive that is never checked against project restrictions. An authenticated remote attacker with instance-creation permission in a restricted project can craft a backup archive where backup.yaml carries restricted settings such as security.privileged=true or raw.lxc directives, bypassing all project restriction enforcement and allowing full host compromise.	9.1	More Details
CVE-2026-32892	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, Chamilo LMS contains an OS Command Injection vulnerability in the file move function. The move() function in fileManage.lib.php passes user-controlled path values directly into exec() shell commands without using escapeshellarg(). When a user moves a document via document.php, the move_to POST parameter — which only passes through Security::remove_XSS() (an HTML-only filter) — is concatenated directly into shell commands such as exec("mv $source $target"). By default, Chamilo allows all authenticated users to create courses (allow_users_to_create_courses = true). Any user who is a teacher in a course (including self-created courses) can move documents, making this vulnerability exploitable by any authenticated user. The attacker must first place a directory with shell metacharacters in its name on the filesystem (achievable via Course Backup Import), then move a document into that directory to trigger arbitrary command execution as the web server user (www-data). This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	9.1	More Details
CVE-2026-34457	OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. Versions prior to 7.15.2 contain a configuration-dependent authentication bypass in deployments where OAuth2 Proxy is used with an auth_request-style integration (such as nginx auth_request) and either --ping-user-agent is set or --gcp-healthchecks is enabled. In affected configurations, OAuth2 Proxy treats any request with the configured health check User-Agent value as a successful health check regardless of the requested path, allowing an unauthenticated remote attacker to bypass authentication and access protected upstream resources. Deployments that do not use auth_request-style subrequests or that do not enable --ping-user-agent/--gcp-healthchecks are not affected. This issue is fixed in 7.15.2.	9.1	More Details
CVE-2026-29145	CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled vulnerability in Apache Tomcat, Apache Tomcat Native. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.1.0-M7 through 10.1.52, from 9.0.83 through 9.0.115; Apache Tomcat Native: from 1.1.23 through 1.1.34, from 1.2.0 through 1.2.39, from 1.3.0 through 1.3.6, from 2.0.0 through 2.0.13. Users are recommended to upgrade to version Tomcat Native 1.3.7 or 2.0.14 and Tomcat 11.0.20, 10.1.53 and 9.0.116, which fix the issue.	9.1	More Details
CVE-2026-5085	Solstice::Session versions through 1440 for Perl generates session ids insecurely. The _generateSessionID method returns an MD5 digest seeded by the epoch time, a random hash reference, a call to the built-in rand() function and the process id. The same method is used in the _generateID method in Solstice::Subsession, which is part of the same distribution. The epoch time may be guessed, if it is not leaked in the HTTP Date header. Stringified hash refences will contain predictable content. The built-in rand() function is seeded by 16-bits and is unsuitable for security purposes. The process id comes from a small set of numbers. Predictable session ids could allow an attacker to gain access to systems.	9.1	More Details
CVE-2026-39912	V2Board 1.6.1 through 1.7.4 and Xboard through 0.1.9 expose authentication tokens in HTTP response bodies of the loginWithMailLink endpoint when the login_with_mail_link_enable feature is active. Unauthenticated attackers can POST to the loginWithMailLink endpoint with a known email address to receive the full authentication URL in the response, then exchange the token at the token2Login endpoint to obtain a valid bearer token with complete account access including admin privileges.	9.1	More Details
CVE-2026-39980	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 6.9.5, the safeEjs.ts file does not properly sanitize EJS templates. Users with the Manage customization capability can run arbitrary JavaScript in the context of the OpenCTI platform process during notifier template execution. This vulnerability is fixed in 6.9.5.	9.1	More Details
CVE-2026-39958	oma is a package manager for AOSC OS. Prior to 1.25.2, oma-topics is responsible for fetching metadata for testing repositories (topics) named "Topic Manifests" ({mirror}/debs/manifest/topics.json) from remote repository servers, registering them as APT source entries. However, the name field in said metadata were not checked for transliteration. In this case, a malicious party may supply a malformed Topic Manifest, which may cause malicious APT source entries to be added to /etc/apt/sources.list.d/atm.list as oma-topics finishes fetching and registering metadata. This vulnerability is fixed in 1.25.2.	9.1	More Details
CVE-2026-30479	A Dynamic-link Library Injection vulnerability in OSGeo Project MapServer before v8.0 allows attackers to execute arbitrary code via a crafted executable.	9.1	More Details
CVE-2026-5445	An out-of-bounds read vulnerability exists in the `DecodeLookupTable` function within `DicomImageDecoder.cpp`. The lookup-table decoding logic used for `PALETTE COLOR` images does not validate pixel indices against the lookup table size. Crafted images containing indices larger than the palette size cause the decoder to read beyond allocated lookup table memory and expose heap contents in the output image.	9.1	More Details

CVE-2026-34179	In Canonical LXD versions 4.12 through 6.7, the doCertificateUpdate function in lxd/certificates.go does not validate the Type field when handling PUT/PATCH requests to /1.0/certificates/{fingerprint} for restricted TLS certificate users, allowing a remote authenticated attacker to escalate privileges to cluster admin.	9.1	More Details
CVE-2025-50228	Jizhicms v2.5.4 is vulnerable to Server-Side Request Forgery (SSRF) in User Evaluation, Message, and Comment modules.	9.1	More Details
CVE-2023-46945	QD 20230821 is vulnerable to Server-side request forgery (SSRF) via a crafted request	9.1	More Details
CVE-2026-31017	A Server-Side Request Forgery (SSRF) vulnerability exists in the Print Format functionality of ERPNext v16.0.1 and Frappe Framework v16.1.1, where user-supplied HTML is insufficiently sanitized before being rendered into PDF. When generating PDFs from user-controlled HTML content, the application allows the inclusion of HTML elements such as <iframe> that reference external resources. The PDF rendering engine automatically fetches these resources on the server side. An attacker can abuse this behavior to force the server to make arbitrary HTTP requests to internal services, including cloud metadata endpoints, potentially leading to sensitive information disclosure.	9.1	More Details
CVE-2026-40035	Unfurl through 2025.08 contains an improper input validation vulnerability in config parsing that enables Flask debug mode by default. The debug configuration value is read as a string and passed directly to app.run(), causing any non-empty string to evaluate truthy, allowing attackers to access the Werkzeug debugger and disclose sensitive information or achieve remote code execution.	9.1	More Details
CVE-2026-40313	PraisonAI is a multi-agent teams system. In versions 4.5.139 and below, the GitHub Actions workflows are vulnerable to ArtiPACKED attack, a known credential leakage vector caused by using actions/checkout without setting persist-credentials: false. By default, actions/checkout writes the GITHUB_TOKEN (and sometimes ACTIONS_RUNTIME_TOKEN) into the .git/config file for persistence, and if any subsequent workflow step uploads artifacts (build outputs, logs, test results, etc.), these tokens can be inadvertently included. Since PraisonAI is a public repository, any user with read access can download these artifacts and extract the leaked tokens, potentially enabling an attacker to push malicious code, poison releases and PyPI/Docker packages, steal repository secrets, and execute a full supply chain compromise affecting all downstream users. The issue spans numerous workflow and action files across .github/workflows/ and .github/actions/. This issue has been fixed in version 4.5.140.	9.1	More Details
CVE-2026-40289	PraisonAI is a multi-agent teams system. In versions below 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents, the browser bridge (praisonai browser start) is vulnerable to unauthenticated remote session hijacking due to missing authentication and a bypassable origin check on its /ws WebSocket endpoint. The server binds to 0.0.0.0 by default and only validates the Origin header when one is present, meaning any non-browser client that omits the header is accepted without restriction. An unauthenticated network attacker can connect, send a start_session message, and the server will route it to the first idle browser-extension WebSocket (effectively hijacking that session) and then broadcast all resulting automation actions and outputs back to the attacker. This enables unauthorized remote control of connected browser automation sessions, leakage of sensitive page context and automation results, and misuse of model-backed browser actions in any environment where the bridge is network-reachable. This issue has been fixed in versions 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents.	9.1	More Details
CVE-2025-57735	When user logged out, the JWT token the user had authtenticated with was not invalidated, which could lead to reuse of that token in case it was intercepted. In Airflow 3.2 we implemented the mechanism that implements token invalidation at logout. Users who are concerned about the logout scenario and possibility of intercepting the tokens, should upgrade to Airflow 3.2+ Users are recommended to upgrade to version 3.2.0, which fixes this issue.	9.1	More Details
CVE-2026-34177	Canonical LXD versions 4.12 through 6.7 contain an incomplete denylist in isVMLowLevelOptionForbidden (lxd/project/limits/permissions.go), which omits raw.apparmor and raw.qemu.conf from the set of keys blocked under the restricted.virtual-machines.lowlevel=block project restriction. A remote attacker with can_edit permission on a VM instance in a restricted project can inject an AppArmor rule and a QEMU chardev configuration that bridges the LXD Unix socket into the guest VM, enabling privilege escalation to LXD cluster administrator and subsequently to host root.	9.1	More Details
CVE-2026-4365	The LearnPress plugin for WordPress is vulnerable to unauthorized data deletion due to a missing capability check on the `delete_question_answer()` function in all versions up to, and including, 4.3.2.8. The plugin exposes a `wp_rest` nonce in public frontend HTML (`lpData`) to unauthenticated visitors, and uses that nonce as the only security gate for the `lp-load-ajax` AJAX dispatcher. The `delete_question_answer` action has no capability or ownership check. This makes it possible for unauthenticated attackers to delete any quiz answer option by sending a crafted POST request with a publicly available nonce.	9.1	More Details
CVE-2026-39860	Nix is a package manager for Linux and other Unix systems. A bug in the fix for CVE-2024-27297 allowed for arbitrary overwrites of files writable by the Nix process orchestrating the builds (typically the Nix daemon running as root in multi-user installations) by following symlinks during fixed-output derivation output registration. This affects sandboxed Linux builds - sandboxed macOS builds are unaffected. The location of the temporary output used for the output copy was located inside the build chroot. A symlink, pointing to an arbitrary location in the filesystem, could be created by the derivation builder at that path. During output registration, the Nix process (running in the host mount namespace) would follow that symlink and overwrite the destination with the derivation's output contents. In multi-user installations, this allows all users able to submit builds to the Nix daemon (allowed-users - defaulting to all users) to gain root privileges by modifying sensitive files. This vulnerability is fixed in 2.34.5, 2.33.4, 2.32.7, 2.31.4, 2.30.4, 2.29.3, and 2.28.6.	9.0	More Details

CVE-2026-26149	Improper neutralization of escape, meta, or control sequences in Microsoft Power Apps allows an authorized attacker to bypass a security feature over a network.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-70810	Cross Site Request Forgery vulnerability in Phpbb phbb3 v.3.3.15 allows a local attacker to execute arbitrary code via the login function and the authentication mechanism	8.8	More Details
CVE-2026-6016	A vulnerability was found in Tenda AC9 15.03.02.13. The affected element is the function decodePwd of the file /goform/WizardHandle of the component POST Request Handler. Performing a manipulation of the argument WANS results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-6121	A flaw has been found in Tenda F451 1.0.0.7. Affected by this vulnerability is the function WrlclientSet of the file /goform/WrlclientSet of the component httpd. This manipulation of the argument GO causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-6120	A vulnerability was detected in Tenda F451 1.0.0.7. Affected is the function fromDhcpListClient of the file /goform/DhcpListClient of the component httpd. The manipulation of the argument page results in stack-based buffer overflow. The attack can be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-5144	The BuddyPress Groupblog plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.9.3. This is due to the group blog settings handler accepting the `groupblog-blogid`, `default-member`, and `groupblog-silent-add` parameters from user input without proper authorization checks. The `groupblog-blogid` parameter allows any group admin (including Subscribers who create their own group) to associate their group with any blog on the Multisite network, including the main site (blog ID 1). The `default-member` parameter accepts any WordPress role, including `administrator`, without validation against a whitelist. When combined with `groupblog-silent-add`, any user who joins the attacker's group is automatically added to the targeted blog with the injected role. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate any user (including themselves via a second account) to Administrator on the main site of the Multisite network.	8.8	More Details
CVE-2026-32171	Insufficiently protected credentials in Azure Logic Apps allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-33618	Chamilo LMS is a learning management system. Prior to .0.0-RC.3, the PlatformConfigurationController::decodeSettingArray() method uses PHP's eval() to parse platform settings from the database. An attacker with admin access (obtainable via Advisory 1) can inject arbitrary PHP code into the settings, which is then executed when any user (including unauthenticated) requests /platform-config/list. This vulnerability is fixed in 2.0.0-RC.3.	8.8	More Details
CVE-2026-35669	OpenClaw before 2026.3.25 contains a privilege escalation vulnerability in gateway-authenticated plugin HTTP routes that incorrectly mint operator.admin runtime scope regardless of caller-granted scopes. Attackers can exploit this scope boundary bypass to gain elevated privileges and perform unauthorized administrative actions.	8.8	More Details
CVE-2026-35666	OpenClaw before 2026.3.22 contains an allowlist bypass vulnerability in system.run approvals that fails to unwrap /usr/bin/time wrappers. Attackers can bypass executable binding restrictions by using an unregistered time wrapper to reuse approval state for inner commands.	8.8	More Details
CVE-2026-35663	OpenClaw before 2026.3.25 contains a privilege escalation vulnerability allowing non-admin operators to self-request broader scopes during backend reconnect. Attackers can bypass pairing requirements to reconnect as operator.admin, gaining unauthorized administrative privileges.	8.8	More Details
CVE-2026-35643	OpenClaw before 2026.3.22 contains an unvalidated WebView JavascriptInterface vulnerability allowing attackers to inject arbitrary instructions. Untrusted pages can invoke the canvas bridge to execute malicious code within the Android application context.	8.8	More Details
CVE-2026-23780	An issue was discovered in BMC Control-M/MFT 9.0.20 through 9.0.22. A SQL injection vulnerability in the MFT API's debug interface allows an authenticated attacker to inject malicious queries due to improper input validation and unsafe dynamic SQL handling. Successful exploitation can enable arbitrary file read/write operations and potentially lead to remote code execution.	8.8	More Details
CVE-2026-40217	LiteLLM through 2026-04-08 allows remote attackers to execute arbitrary code via bytecode rewriting at the /guardrails/test_custom_code URI.	8.8	More Details
CVE-2026-6015	A vulnerability has been found in Tenda AC9 15.03.02.13. Impacted is the function formQuickIndex of the file /goform/QuickIndex of the component POST Request Handler. Such manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-	Use after free in WebRTC in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary		More

2026-5860	code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	Details
CVE-2026-39891	PraisonAI is a multi-agent teams system. Prior to 4.5.115, the create_agent_centric_tools() function returns tools (like acp_create_file) that process file content using template rendering. When user input from agent.start() is passed directly into these tools without escaping, template expressions in the input are executed rather than treated as literal text. This vulnerability is fixed in 4.5.115.	8.8	More Details
CVE-2026-6014	A flaw has been found in D-Link DIR-513 1.10. This issue affects the function formAdvanceSetup of the file /goform/formAdvanceSetup of the component POST Request Handler. This manipulation of the argument webpage causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-6013	A vulnerability was detected in D-Link DIR-513 1.10. This vulnerability affects the function formSetRoute of the file /goform/formSetRoute of the component POST Request Handler. The manipulation of the argument curTime results in buffer overflow. The attack may be performed from remote. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-6012	A security vulnerability has been detected in D-Link DIR-513 1.10. This affects the function formSetPassword of the file /goform/formSetPassword of the component POST Request Handler. The manipulation of the argument curTime leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5992	A vulnerability was determined in Tenda F451 1.0.0.7. This affects the function fromP2pListFilter of the file /goform/P2pListFilter. This manipulation of the argument page causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-5991	A vulnerability was found in Tenda F451 1.0.0.7. Affected by this issue is the function formWrlExtraSet of the file /goform/WrlExtraSet. The manipulation of the argument GO results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-5990	A vulnerability has been found in Tenda F451 1.0.0.7. Affected by this vulnerability is the function fromSafeEmailFilter of the file /goform/SafeEmailFilter. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-5989	A flaw has been found in Tenda F451 1.0.0.7. Affected is the function fromRouteStatic of the file /goform/RouteStatic. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2026-26178	Integer size truncation in Windows Advanced Rasterization Platform (WARP) allows an unauthorized attacker to elevate privileges locally.	8.8	More Details
CVE-2026-5988	A vulnerability was detected in Tenda F451 1.0.0.7. This impacts the function formWrlsafeset of the file /goform/AdvSetWrlsafeset. Performing a manipulation of the argument mit_ssid results in stack-based buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-5858	Heap buffer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-6122	A vulnerability has been found in Tenda F451 1.0.0.7. Affected by this issue is the function frmL7ProtForm of the file /goform/L7Prot of the component httpd. Such manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-6123	A vulnerability was found in Tenda F451 1.0.0.7. This affects the function fromAddressNat of the file /goform/addressNat of the component httpd. Performing a manipulation of the argument entrys results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-6124	A vulnerability was determined in Tenda F451 1.0.0.7. This vulnerability affects the function fromSafeMacFilter of the file /goform/SafeMacFilter of the component httpd. Executing a manipulation of the argument page/menufacturer can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-6133	A vulnerability was identified in Tenda F451 1.0.0.7_cn_svn7958. This affects the function fromSafeUrlFilter of the file /goform/SafeUrlFilter. Such manipulation of the argument page leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-26167	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	8.8	More Details
CVE-2026-39815	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiDDoS-F 7.2.1 through 7.2.2 may allow attacker to execute unauthorized code or commands via sending crafted HTTP requests	8.8	More Details
CVE-2026-	A Broken Object-Level Authorization (BOLA) in the /Settings/UserController.php endpoint of Webkul Krayin CRM v2.2.x allows authenticated attackers to arbitrarily reset user passwords and perform a full account takeover via supplying a	8.8	More Details

38529	crafted HTTP request.		
CVE-2026-27668	A vulnerability has been identified in RUGGEDCOM CROSSBOW Secure Access Manager Primary (SAM-P) (All versions < V5.8). User Administrators are allowed to administer groups they belong to. This could allow an authenticated User Administrator to escalate their own privileges and grant themselves access to any device group at any access level.	8.8	More Details
CVE-2026-25654	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP3). Affected products do not properly validate user authorization when processing password reset requests. This could allow an authenticated remote attacker to bypass authorization checks, leading to the ability to reset the password of any arbitrary user account.	8.8	More Details
CVE-2026-6200	A vulnerability was determined in Tenda F456 1.0.0.5. The affected element is the function formwebtypelibrary of the file /goform/webtypelibrary. This manipulation of the argument menufacturer/Go causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-6199	A vulnerability was found in Tenda F456 1.0.0.5. Impacted is the function fromqossetting of the file /goform/qossetting. The manipulation of the argument page results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-6198	A vulnerability has been found in Tenda F456 1.0.0.5. This issue affects the function fromNatStaticSetting of the file /goform/NatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-6197	A flaw has been found in Tenda F456 1.0.0.5. This vulnerability affects the function formWrlsafeset of the file /goform/AdvSetWrlsafeset. Executing a manipulation of the argument mit_ssid can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been published and may be used.	8.8	More Details
CVE-2026-40040	Pachno 1.0.6 contains an unrestricted file upload vulnerability that allows authenticated users to upload arbitrary file types by bypassing ineffective extension filtering to the /uploadfile endpoint. Attackers can upload executable files .php5 scripts to web-accessible directories and execute them to achieve remote code execution on the server.	8.8	More Details
CVE-2026-6196	A vulnerability was detected in Tenda F456 1.0.0.5. This affects the function fromexeCommand of the file /goform/exeCommand. Performing a manipulation of the argument cmdinput results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-6194	A weakness has been identified in Totolink A3002MU B20211125.1046. Affected by this vulnerability is the function sub_410188 of the file /boafrm/formWlanSetup of the component HTTP Request Handler. This manipulation of the argument wan-url causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-6186	A security vulnerability has been detected in UTT HiPER 1200GW up to 2.5.3-170306. This vulnerability affects the function strcpy of the file /goform/formNatStaticMap. The manipulation of the argument NatBind leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2026-33858	Dag Authors, who normally should not be able to execute code in the webserver context could craft XCom payload causing the webserver to execute arbitrary code. Since Dag Authors are already highly trusted, severity of this issue is Low. Users are recommended to upgrade to Apache Airflow 3.2.0, which resolves this issue.	8.8	More Details
CVE-2026-35337	Deserialization of Untrusted Data vulnerability in Apache Storm. Versions Affected: before 2.8.6. Description: When processing topology credentials submitted via the Nimbus Thrift API, Storm deserializes the base64-encoded TGT blob using ObjectInputStream.readObject() without any class filtering or validation. An authenticated user with topology submission rights could supply a crafted serialized object in the "TGT" credential field, leading to remote code execution in both the Nimbus and Worker JVMs. Mitigation: 2.x users should upgrade to 2.8.6. Users who cannot upgrade immediately should monkey-patch an ObjectInputFilter allow-list to ClientAuthUtils.deserializeKerberosTicket() restricting deserialized classes to javax.security.auth.kerberos.KerberosTicket and its known dependencies. A guide on how to do this is available in the release notes of 2.8.6. Credit: This issue was discovered by K.	8.8	More Details
CVE-2026-6168	A flaw has been found in TOTOLINK A7000R up to 9.1.0u.6115. The affected element is the function setWiFiEasyGuestCfg of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument ssid5g causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2026-6157	A vulnerability was detected in Totolink A800R 4.1.2cu.5137_B20200730. This impacts the function setAppEasyWizardConfig in the library /lib/cste_modules/app.so. The manipulation of the argument apcliSsid results in buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-3243	The Advanced Members for ACF plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the create_crop function in all versions up to, and including, 1.2.5. 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 vulnerability was partially patched in version 1.2.5.	8.8	More Details
CVE-2026-6137	A vulnerability was detected in Tenda F451 1.0.0.7_cn_svn7958. The affected element is the function fromAdvSetWan of the file /goform/AdvSetWan. The manipulation of the argument wanmode/PPPOEPassword results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2026-6136	A security vulnerability has been detected in Tenda F451 1.0.0.7_cn_svn7958. Impacted is the function frmL7ImForm of the file /goform/L7Im. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	8.8	More Details

CVE-2026-6135	A weakness has been identified in Tenda F451 1.0.0.7_cn_svn7958. This issue affects the function fromSetIpBind of the file /goform/SetIpBind. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-6134	A security flaw has been discovered in Tenda F451 1.0.0.7_cn_svn7958. This vulnerability affects the function fromqossetting of the file /goform/qossetting. Performing a manipulation of the argument qos results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-32157	Use after free in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-5859	Integer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-32225	Protection mechanism failure in Windows Shell allows an unauthorized attacker to bypass a security feature over a network.	8.8	More Details
CVE-2026-5861	Use after free in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5912	Integer overflow in WebRTC in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2026-5980	A flaw has been found in D-Link DIR-605L 2.13B01. Affected by this issue is the function formSetMACFilter of the file /goform/formSetMACFilter of the component POST Request Handler. This manipulation of the argument curTime causes buffer overflow. The attack may be initiated remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5862	Inappropriate implementation in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5904	Use after free in V8 in Google Chrome prior to 147.0.7727.55 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Low)	8.8	More Details
CVE-2026-35196	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, an OS Command Injection vulnerability exists in the main/inc/ajax/gradebook.ajax.php endpoint within the export_all_certificates action, where the course code retrieved from the session variable $_SESSION['_cid'] via api_get_course_id() is concatenated directly into a shell_exec() command string without sanitization or escaping using escapeshellarg(). If an attacker can manipulate or poison their session data to inject shell metacharacters into the _cid variable, they can achieve arbitrary command execution on the underlying server. Successful exploitation grants full access to read system files and credentials, alters the application and database, or disrupts server availability. This issue has been fixed in version 2.0.0-RC.3.	8.8	More Details
CVE-2026-40291	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, an insecure direct object modification vulnerability in the PUT /api/users/{id} endpoint allows any authenticated user with ROLE_STUDENT to escalate their privileges to ROLE_ADMIN by modifying the roles field on their own user record. The API Platform security expression is_granted('EDIT', object) only verifies record ownership, and the roles field is included in the writable serialization group, enabling any user to set arbitrary roles such as ROLE_ADMIN. Successful exploitation grants full administrative control of the platform, including access to all courses, user data, grades, and administrative settings. This issue has been fixed in version 2.0.0-RC.3.	8.8	More Details
CVE-2026-5908	Integer overflow in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-5909	Integer overflow in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-5910	Integer overflow in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: Low)	8.8	More Details
CVE-2026-	The Product Feed PRO for WooCommerce by AdTribes – Product Feeds for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions 13.4.6 through 13.5.2.1. This is due to missing or incorrect nonce validation on the ajax_migrate_to_custom_post_type, ajax_adt_clear_custom_attributes_product_meta_keys, ajax_update_file_url_to_lower_case, ajax_use_legacy_filters_and_rules, and ajax_fix_duplicate_feed functions. This	8.8	More

3499	makes it possible for unauthenticated attackers to trigger feed migration, clear custom-attribute transient caches, rewrite feed file URLs to lowercase, toggle legacy filter and rule settings, and delete duplicated feed posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.		Details
CVE-2026-5914	Type Confusion in CSS in Google Chrome prior to 147.0.7727.55 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Low)	8.8	More Details
CVE-2026-35638	OpenClaw before 2026.3.22 contains a privilege escalation vulnerability in the Control UI that allows unauthenticated sessions to retain self-declared privileged scopes without device identity verification. Attackers can exploit the device-less allow path in the trusted-proxy mechanism to maintain elevated permissions by declaring arbitrary scopes, bypassing device identity requirements.	8.8	More Details
CVE-2026-5815	A vulnerability was detected in D-Link DIR-645 1.01/1.02/1.03. Impacted is the function hedwigcgi_main of the file /cgi-bin/hedwig.cgi. The manipulation results in stack-based buffer overflow. The attack can be launched remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-4326	The Vertex Addons for Elementor plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 1.6.4. This is due to improper authorization enforcement in the activate_required_plugins() function. Specifically, the current_user_can('install_plugins') capability check does not terminate execution when it fails — it only sets an error message variable while allowing the plugin installation and activation code to execute. The error response is only sent after the installation and activation have already completed. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate arbitrary plugins from the WordPress.	8.8	More Details
CVE-2026-5830	A vulnerability was identified in Tenda AC15 15.03.05.18. This affects the function websGetVar of the file /goform/SysToolChangePwd. Such manipulation of the argument oldPwd/newPwd/cfmPwd leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-27140	SWIG file names containing 'cgo' and well-crafted payloads could lead to code smuggling and arbitrary code execution at build time due to trust layer bypass.	8.8	More Details
CVE-2026-39981	AGiXT is a dynamic AI Agent Automation Platform. Prior to 1.9.2, the safe_join() function in the essential_abilities extension fails to validate that resolved file paths remain within the designated agent workspace. An authenticated attacker can use directory traversal sequences to read, write, or delete arbitrary files on the server hosting the AGiXT instance. This vulnerability is fixed in 1.9.2.	8.8	More Details
CVE-2026-3357	IBM Langflow Desktop 1.6.0 through 1.8.2 Langflow could allow an authenticated user to execute arbitrary code on the system, caused by an insecure default setting which permits the deserialization of untrusted data in the FAISS component.	8.8	More Details
CVE-2026-39911	Hashgraph Guardian through version 3.5.0 contains an unsandboxed JavaScript execution vulnerability in the Custom Logic policy block worker that allows authenticated Standard Registry users to execute arbitrary code by passing user-supplied JavaScript expressions directly to the Node.js Function() constructor without isolation. Attackers can import native Node.js modules to read arbitrary files from the container filesystem, access process environment variables containing sensitive credentials such as RSA private keys, JWT signing keys, and API tokens, and forge valid authentication tokens for any user including administrators.	8.8	More Details
CVE-2026-30478	A Dynamic-link Library Injection vulnerability in GatewayGeo MapServer for Windows version 5 allows attackers to escalate privileges via a crafted executable.	8.8	More Details
CVE-2025-70364	An issue was discovered in Kiamo before 8.4 allowing authenticated administrative attackers to execute arbitrary PHP code on the server.	8.8	More Details
CVE-2026-33785	A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on MX Series allows a local, authenticated user with low privileges to execute specific commands which will lead to a complete compromise of managed devices. Any user logged in, without requiring specific privileges, can issue 'request csds' CLI operational commands. These commands are only meant to be executed by high privileged or users designated for Juniper Device Manager (JDM) / Connected Security Distributed Services (CSDS) operations as they will impact all aspects of the devices managed via the respective MX. This issue affects Junos OS on MX Series: * 24.4 releases before 24.4R2-S3, * 25.2 releases before 25.2R2. This issue does not affect Junos OS releases before 24.4.	8.8	More Details
CVE-2026-5979	A vulnerability was detected in D-Link DIR-605L 2.13B01. Affected by this vulnerability is the function formVirtualServ of the file /goform/formVirtualServ of the component POST Request Handler. The manipulation of the argument curTime results in buffer overflow. The attack can be launched remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5870	Integer overflow in Skia in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-	A vulnerability has been found in D-Link DIR-605L 2.13B01. This affects the function formAdvFirewall of the file		

2026-5981	/goform/formAdvFirewall of the component POST Request Handler. Such manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5863	Inappropriate implementation in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-33120	Untrusted pointer dereference in SQL Server allows an authorized attacker to execute code over a network.	8.8	More Details
CVE-2026-5984	A vulnerability was identified in D-Link DIR-605L 2.13B01. Impacted is the function formSetLog of the file /goform/formSetLog of the component POST Request Handler. The manipulation of the argument curTime leads to buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5865	Type Confusion in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5866	Use after free in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5983	A vulnerability was determined in D-Link DIR-605L 2.13B01. This issue affects the function formSetDDNS of the file /goform/formSetDDNS of the component POST Request Handler. Executing a manipulation of the argument curTime can lead to buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5868	Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5982	A vulnerability was found in D-Link DIR-605L 2.13B01. This vulnerability affects the function formAdvNetwork of the file /goform/formAdvNetwork of the component POST Request Handler. Performing a manipulation of the argument curTime results in buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2026-5871	Type Confusion in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5872	Use after free in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-5873	Out of bounds read and write in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-39621	Cross-Site Request Forgery (CSRF) vulnerability in spicethemes SpicePress spicepress allows Upload a Web Shell to a Web Server.This issue affects SpicePress: from n/a through <= 2.3.2.5.	8.8	More Details
CVE-2026-5877	Use after free in Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-5879	Insufficient validation of untrusted input in ANGLE in Google Chrome on Mac prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-24893	openITCOCKPIT is an open source monitoring tool built for different monitoring engines. openITCOCKPIT Community Edition prior to version 5.5.2 contains a command injection vulnerability that allows an authenticated user with permission to add or modify hosts to execute arbitrary OS commands on the monitoring backend. The vulnerability arises because user-controlled host attributes (specifically the host address) are expanded into monitoring command templates without validation, escaping, or quoting. These templates are later executed by the monitoring engine (Nagios/Icinga) via a shell, resulting in remote code execution. Version 5.5.2 patches the issue.	8.8	More Details
CVE-2026-5884	Insufficient validation of untrusted input in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-35639	OpenClaw before 2026.3.22 contains a privilege escalation vulnerability in the device.pair.approve method that allows an operator.pairing approver to approve pending device requests with broader operator scopes than the approver actually holds. Attackers can exploit insufficient scope validation to escalate privileges to operator.admin and achieve remote code execution on the Node infrastructure.	8.8	More Details

CVE-2026-35169	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From to before 27.0.3 and 28.0.1, the help_editor module of LORIS did not properly sanitize some user supplied variables which could result in a reflected cross-site scripting attack if a user is tricked into following an invalid link. The same input vector could also allow an attacker to download arbitrary markdown files on an unpatched server. This vulnerability is fixed in 27.0.3 and 28.0.1.	8.7	More Details
CVE-2026-27928	Improper input validation in Windows Hello allows an unauthorized attacker to bypass a security feature over a network.	8.7	More Details
CVE-2025-13914	A Key Exchange without Entity Authentication vulnerability in the SSH implementation of Juniper Networks Apstra allows a unauthenticated, MITM attacker to impersonate managed devices. Due to insufficient SSH host key validation an attacker can perform a machine-in-the-middle attack on the SSH connections from Apstra to managed devices, enabling an attacker to impersonate a managed device and capture user credentials. This issue affects all versions of Apstra before 6.1.1.	8.7	More Details
CVE-2026-34617	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could result in privilege escalation. A low-privileged attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	8.7	More Details
CVE-2026-34160	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, the PENS (Package Exchange Notification Services) plugin endpoint at public/plugin/Pens/pens.php is accessible without authentication and accepts a user-controlled package-url parameter that the server fetches using curl without filtering private or internal IP addresses, enabling unauthenticated Server-Side Request Forgery (SSRF). An attacker can exploit this to probe internal network services, access cloud metadata endpoints (such as 169.254.169.254) to steal IAM credentials and sensitive instance metadata, or trigger state-changing operations on internal services via the receipt and alerts callback parameters. No authentication is required to exploit either SSRF vector, significantly increasing the attack surface. This issue has been fixed in version 2.0.0-RC.3.	8.6	More Details
CVE-2026-34622	Acrobat Reader versions 26.001.21411, 24.001.30360, 24.001.30362 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') 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.	8.6	More Details
CVE-2026-34621	Acrobat Reader versions 24.001.30356, 26.001.21367 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') 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.	8.6	More Details
CVE-2026-27305	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue does not require user interaction.	8.6	More Details
CVE-2026-4436	A low-privileged remote attacker can send Modbus packets to manipulate register values that are inputs to the odorant injection logic such that too much or too little odorant is injected into a gas line.	8.6	More Details
CVE-2026-40158	PraisonAI is a multi-agent teams system. Prior to 4.5.128, PraisonAI's AST-based Python sandbox can be bypassed using type.__getattribute__ trampoline, allowing arbitrary code execution when running untrusted agent code. The _execute_code_direct function in praisonaiagents/tools/python_tools.py uses AST filtering to block dangerous Python attributes like __subclasses__, __globals__, and __bases__. However, the filter only checks ast.Attribute nodes, allowing a bypass. The sandbox relies on AST-based filtering of attribute access but fails to account for dynamic attribute resolution via built-in methods such as type.getattribute, resulting in incomplete enforcement of security restrictions. The string '__subclasses__' is an ast.Constant, not an ast.Attribute, so it is never checked against the blocked list. This vulnerability is fixed in 4.5.128.	8.6	More Details
CVE-2026-39983	basic-ftp is an FTP client for Node.js. Prior to 5.2.1, basic-ftp allows FTP command injection via CRLF sequences (\r\n) in file path parameters passed to high-level path APIs such as cd(), remove(), rename(), uploadFrom(), downloadTo(), list(), and removeDir(). The library's protectWhitespace() helper only handles leading spaces and returns other paths unchanged, while FtpContext.send() writes the resulting command string directly to the control socket with \r\n appended. This lets attacker-controlled path strings split one intended FTP command into multiple commands. This vulnerability is fixed in 5.2.1.	8.6	More Details
CVE-2026-27290	Adobe Framemaker versions 2022.8 and earlier are affected by an Untrusted Search Path vulnerability that might allow attackers to execute arbitrary code in the context of the current user. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue does not require user interaction.	8.6	More Details
CVE-2026-3830	The Product Filter for WooCommerce by WBW WordPress plugin before 3.1.3 does not sanitize and escape a parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection attacks	8.6	More Details

CVE-2026-5329	Rapid7 Velociraptor versions prior to 0.76.2 contain an improper input validation vulnerability in the client monitoring message handler on the Velociraptor server (primarily Linux) that allows an authenticated remote attacker to write to arbitrary internal server queues via a crafted monitoring message with a malicious queue name. The server handler that receives client monitoring messages does not sufficiently validate the queue name supplied by the client, allowing a rogue client to write arbitrary messages to privileged internal queues. This may lead to remote code execution on the Velociraptor server. Rapid7 Hosted Velociraptor instances are not affected by this vulnerability.	8.5	More Details
CVE-2026-38527	A Server-Side Request Forgery (SSRF) in the /settings/webhooks/create component of Webkul Krayin CRM v2.2.x allows attackers to scan internal resources via supplying a crafted POST request.	8.5	More Details
CVE-2026-39974	n8n-MCP is a Model Context Protocol (MCP) server that provides AI assistants with comprehensive access to n8n node documentation, properties, and operations. Prior to 2.47.4, an authenticated Server-Side Request Forgery in n8n-mcp allows a caller holding a valid AUTH_TOKEN to cause the server to issue HTTP requests to arbitrary URLs supplied through multi-tenant HTTP headers. Response bodies are reflected back through JSON-RPC, so an attacker can read the contents of any URL the server can reach — including cloud instance metadata endpoints (AWS IMDS, GCP, Azure, Alibaba, Oracle), internal network services, and any other host the server process has network access to. The primary at-risk deployments are multi-tenant HTTP installations where more than one operator can present a valid AUTH_TOKEN, or where a token is shared with less-trusted clients. Single-tenant stdio deployments and HTTP deployments without multi-tenant headers are not affected. This vulnerability is fixed in 2.47.4.	8.5	More Details
CVE-2026-39942	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.17.0, the PATCH /files/{id} endpoint accepts a user-controlled filename_disk parameter. By setting this value to match the storage path of another user's file, an attacker can overwrite that file's content while manipulating metadata fields such as uploaded_by to obscure the tampering. This vulnerability is fixed in 11.17.0.	8.5	More Details
CVE-2026-5936	An attacker can control a server-side HTTP request by supplying a crafted URL, causing the server to initiate requests to arbitrary destinations. This behavior may be exploited to probe internal network services, access otherwise unreachable endpoints (e.g., cloud metadata services), or bypass network access controls, potentially leading to sensitive information disclosure and further compromise of the internal environment.	8.5	More Details
CVE-2026-5173	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.9.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user to invoke unintended server-side methods through websocket connections due to improper access control.	8.5	More Details
CVE-2026-5483	A flaw was found in odh-dashboard in Red Hat Openshift AI. This vulnerability in the `odh-dashboard` component of Red Hat OpenShift AI (RHOAI) allows for the disclosure of Kubernetes Service Account tokens through a NodeJS endpoint. This could enable an attacker to gain unauthorized access to Kubernetes resources.	8.5	More Details
CVE-2026-1342	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated user to execute malicious scripts from outside of its control sphere.	8.5	More Details
CVE-2026-39495	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Blind SQL Injection.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.9.27.	8.5	More Details
CVE-2026-39475	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Syed Balkhi User Feedback userfeedback-lite allows Blind SQL Injection.This issue affects User Feedback: from n/a through <= 1.10.1.	8.5	More Details
CVE-2019-25689	HTML5 Video Player 1.2.5 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying an oversized key code string. Attackers can craft a malicious payload exceeding 997 bytes and paste it into the KEY CODE field in the Help Register dialog to trigger code execution and spawn a calculator process.	8.4	More Details
CVE-2019-25691	Faleemi Desktop Software 1.8 contains a local buffer overflow vulnerability in the System Setup dialog that allows attackers to bypass DEP protections through structured exception handling exploitation. Attackers can inject a crafted payload into the Save Path for Snapshot and Record file field to trigger a buffer overflow and execute arbitrary code via ROP chain gadgets.	8.4	More Details
CVE-2026-40113	PraisonAI is a multi-agent teams system. Prior to 4.5.128, deploy.py constructs a single comma-delimited string for the gcloud run deploy --set-env-vars argument by directly interpolating openai_model, openai_key, and openai_base without validating that these values do not contain commas. gcloud uses a comma as the key-value pair separator for --set-env-vars. A comma in any of the three values causes gcloud to parse the trailing text as additional KEY=VALUE definitions, injecting arbitrary environment variables into the deployed Cloud Run service. This vulnerability is fixed in 4.5.128.	8.4	More Details
CVE-2026-40287	PraisonAI is a multi-agent teams system. Versions 4.5.138 and below are vulnerable to arbitrary code execution through automatic, unsanitized import of a tools.py file from the current working directory. Components including call.py (import_tools_from_file()), tool_resolver.py (_load_local_tools()), and CLI tool-loading paths blindly import ./tools.py at startup without any validation, sandboxing, or user confirmation. An attacker who can place a malicious tools.py in the directory where PraisonAI is launched (such as through a shared project, cloned repository, or writable workspace) achieves immediate arbitrary Python code execution in the host environment. This compromises the full PraisonAI process, the host system, and any connected data or credentials. This issue has been fixed in version 4.5.139.	8.4	More Details
CVE-			

2026-33115	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-33114	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-32221	Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2026-27306	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Attacker requires elevated privileges. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	8.4	More Details
CVE-2026-32162	Acceptance of extraneous untrusted data with trusted data in Windows COM allows an unauthorized attacker to elevate privileges locally.	8.4	More Details
CVE-2025-69627	Nitro PDF Pro for Windows 14.41.1.4 contains a heap use-after-free vulnerability in the implementation of the JavaScript method this.mailDoc(). During execution, an internal XID object is allocated and then freed prematurely, after which the freed pointer is still passed into UI and logging helper functions. Because the freed memory region may contain unpredictable heap data or remnants of attacker-controlled JavaScript strings, downstream routines such as wcscmp() may process invalid or stale pointers. This can result in access violations and non-deterministic crashes.	8.4	More Details
CVE-2026-32190	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	8.4	More Details
CVE-2018-25258	RGui 3.5.0 contains a local buffer overflow vulnerability in the GUI preferences dialog that allows attackers to bypass DEP protections through structured exception handling exploitation. Attackers can craft malicious input in the Language for menus and messages field to trigger a stack-based buffer overflow, execute a ROP chain for VirtualAlloc allocation, and achieve arbitrary code execution.	8.4	More Details
CVE-2026-32091	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	8.4	More Details
CVE-2019-25695	R 3.4.4 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by injecting malicious input into the GUI Preferences language field. Attackers can craft a payload with a 292-byte offset and JMP ESP instruction to execute commands like calc.exe when the payload is pasted into the Language for menus and messages field.	8.4	More Details
CVE-2019-25701	Easy Video to iPod Converter 1.6.20 contains a local buffer overflow vulnerability in the user registration field that allows local attackers to overwrite the structured exception handler. Attackers can input a crafted payload exceeding 996 bytes in the username field to trigger SEH overwrite and execute arbitrary code with user privileges.	8.4	More Details
CVE-2026-4788	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.37 stores sensitive information in log files that could be read by a local user.	8.4	More Details
CVE-2019-25705	Echo Mirage 3.1 contains a stack buffer overflow vulnerability that allows local attackers to crash the application or execute arbitrary code by supplying an oversized string in the Rules action field. Attackers can create a malicious text file with a crafted payload exceeding buffer boundaries and paste it into the action field through the Rules dialog to trigger the overflow and overwrite the return address.	8.4	More Details
CVE-2026-31939	Chamilo LMS is a learning management system. Prior to 1.11.38, there is a path traversal in main/exercise/savescores.php leading to arbitrary file feletion. User input from $_REQUEST['test'] is concatenated directly into filesystem path without canonicalization or traversal checks. This vulnerability is fixed in 1.11.38.	8.3	More Details
CVE-2026-35478	InvenTree is an Open Source Inventory Management System. From 0.16.0 to before 1.2.7, any authenticated InvenTree user can create a valid API token attributed to any other user in the system — including administrators and superusers — by supplying the target's user ID in the user field of a POST /api/user/tokens/ request. The returned token is immediately usable for full API authentication as the target user, from any network location, with no further interaction required. This vulnerability is fixed in 1.2.7 and 1.3.0.	8.3	More Details
CVE-2026-35595	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the CanUpdate check at pkg/models/project_permissions.go:139-148 only requires CanWrite on the new parent project when changing parent_project_id. However, Vikunja's permission model uses a recursive CTE that walks up the project hierarchy to compute permissions. Moving a project under a different parent changes the permission inheritance chain. When a user has inherited Write access (from a parent project share) and reparents the child project under their own project tree, the CTE resolves their ownership of the new parent as Admin (permission level 2) on the moved project. This vulnerability is fixed in 2.3.0.	8.3	More Details
CVE-2026-	kcp is a Kubernetes-like control plane for form-factors and use-cases beyond Kubernetes and container workloads. Prior to 0.30.3 and 0.29.3, the cache server is directly exposed by the root shard and has no authentication or authorization in place. This allows anyone who can access the root shard to read and write to the cache server. This	8.2	More Details

39429	vulnerability is fixed in 0.30.3 and 0.29.3.		
CVE-2026-5208	Command injection in alerts in CoolerControl/coolercontrold <4.0.0 allows authenticated attackers to execute arbitrary code as root via injected bash commands in alert names	8.2	More Details
CVE-2023-54359	WordPress adivaha Travel Plugin 2.3 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'pid' GET parameter. Attackers can send requests to the /mobile-app/v3/ endpoint with crafted 'pid' values using XOR-based payloads to extract sensitive database information or cause denial of service.	8.2	More Details
CVE-2026-40168	Postiz is an AI social media scheduling tool. Prior to 2.21.5, the /api/public/stream endpoint is vulnerable to SSRF. Although the application validates the initially supplied URL and blocks direct private/internal hosts, it does not re-validate the final destination after HTTP redirects. As a result, an attacker can supply a public HTTPS URL that passes validation and then redirects the server-side request to an internal resource.	8.2	More Details
CVE-2019-25697	CMSsite 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cat_id parameter. Attackers can send GET requests to category.php with malicious cat_id values to extract sensitive database information including usernames and credentials.	8.2	More Details
CVE-2026-40163	Saltcorn is an extensible, open source, no-code database application builder. Prior to 1.4.5, 1.5.5, and 1.6.0-beta.4, the POST /sync/offline_changes endpoint allows an unauthenticated attacker to create arbitrary directories and write a changes.json file with attacker-controlled JSON content anywhere on the server filesystem. The GET /sync/upload_finished endpoint allows an unauthenticated attacker to list arbitrary directory contents and read specific JSON files. This vulnerability is fixed in 1.4.5, 1.5.5, and 1.6.0-beta.4.	8.2	More Details
CVE-2019-25710	Dolibarr ERP-CRM 8.0.4 contains an SQL injection vulnerability in the rowid parameter of the admin dict.php endpoint that allows attackers to execute arbitrary SQL queries. Attackers can inject malicious SQL code through the rowid POST parameter to extract sensitive database information using error-based SQL injection techniques.	8.2	More Details
CVE-2026-34578	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.6, OPNsense's LDAP authentication connector passes the login username directly into an LDAP search filter without calling ldap_escape(). An unauthenticated attacker can inject LDAP filter metacharacters into the username field of the WebGUI login page to enumerate valid LDAP usernames in the configured directory. When the LDAP server configuration includes an Extended Query to restrict login to members of a specific group, the same injection can be used to bypass that group membership restriction and authenticate as any LDAP user whose password is known, regardless of group membership. This vulnerability is fixed in 26.1.6.	8.2	More Details
CVE-2026-32316	jq is a command-line JSON processor. An integer overflow vulnerability exists through version 1.8.1 within the jvp_string_append() and jvp_string_copy_replace_bad functions, where concatenating strings with a combined length exceeding 2^31 bytes causes a 32-bit unsigned integer overflow in the buffer allocation size calculation, resulting in a drastically undersized heap buffer. Subsequent memory copy operations then write the full string data into this undersized buffer, causing a heap buffer overflow classified as CWE-190 (Integer Overflow) leading to CWE-122 (Heap-based Buffer Overflow). Any system evaluating untrusted jq queries is affected, as an attacker can crash the process or potentially achieve further exploitation through heap corruption by crafting queries that produce extremely large strings. The root cause is the absence of string size bounds checking, unlike arrays and objects which already have size limits. The issue has been addressed in commit e47e56d226519635768e6aab2f38f0ab037c09e5.	8.2	More Details
CVE-2026-22828	A heap-based buffer overflow vulnerability in Fortinet FortiAnalyzer Cloud 7.6.2 through 7.6.4, FortiManager Cloud 7.6.2 through 7.6.4 may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. Successful exploitation would require a large amount of effort in preparation because of ASLR and network segmentation	8.1	More Details
CVE-2026-33827	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-40200	An issue was discovered in musl libc 0.7.10 through 1.2.6. Stack-based memory corruption can occur during qsort of very large arrays, due to incorrectly implemented double-word primitives. The number of elements must exceed about seven million, i.e., the 32nd Leonardo number on 32-bit platforms (or the 64th Leonardo number on 64-bit platforms, which is not practical).	8.1	More Details
CVE-2025-58913	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CactusThemes VideoPro allows PHP Local File Inclusion.This issue affects VideoPro: from n/a through 2.3.8.1.	8.1	More Details
CVE-2026-5436	The MW WP Form plugin for WordPress is vulnerable to Arbitrary File Move/Read in all versions up to and including 5.1.1. This is due to insufficient validation of the $name parameter (upload field key) passed to the generate_user_file_dirpath() function, which uses WordPress's path_join() — a function that returns absolute paths unchanged, discarding the intended base directory. The attacker-controlled key is injected via the mwf_upload_files[] POST parameter, which is loaded into the plugin's Data model via _set_request_valiables(). During form processing, regenerate_upload_file_keys() iterates over these keys and calls generate_user_filepath() with the attacker-supplied key as the $name argument — the key survives validation because the targeted file (e.g., wp-config.php) genuinely exists at the absolute path. The _get_attachments() method then re-reads the same surviving keys and passes the resolved file path to move_temp_file_to_upload_dir(), which calls rename() to move the file into the uploads folder. This makes it possible for unauthenticated attackers to move arbitrary files on the server, which can easily lead to	8.1	More Details

	remote code execution when the right file is moved (such as wp-config.php). The vulnerability is only exploitable if a file upload field is added to the form and the “Saving inquiry data in database” option is enabled.		
CVE-2021-47961	A plaintext storage of a password vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access or influence the user's PIN code due to insecure storage. This may lead to unauthorized VPN configuration and potential interception of subsequent VPN traffic when combined with user interaction.	8.1	More Details
CVE-2026-35660	OpenClaw before 2026.3.23 contains an insufficient access control vulnerability in the Gateway agent /reset endpoint that allows callers with operator.write permission to reset admin sessions. Attackers with operator.write privileges can invoke /reset or /new messages with an explicit sessionKey to bypass operator.admin requirements and reset arbitrary sessions.	8.1	More Details
CVE-2026-35653	OpenClaw before 2026.3.24 contains an incorrect authorization vulnerability in the POST /reset-profile endpoint that allows authenticated callers with operator.write access to browser.request to bypass profile mutation restrictions. Attackers can invoke POST /reset-profile through the browser.request surface to stop the running browser, close Playwright connections, and move profile directories to Trash, crossing intended privilege boundaries.	8.1	More Details
CVE-2026-4351	The Perfmatters plugin for WordPress is vulnerable to arbitrary file overwrite via path traversal in all versions up to, and including, 2.5.9. This is due to the `PMCS::action_handler()` method processing the bulk action `activate`/`deactivate` handlers without any authorization check or nonce verification. The `$_GET['snippets'][]` values are passed unsanitized to `Snippet::activate()`/`Snippet::deactivate()` which call `Snippet::update()` then `file_put_contents()` with the traversed path. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite arbitrary files on the server with a fixed PHP docblock content, potentially causing denial of service by corrupting critical files like `.htaccess` or `index.php`.	8.1	More Details
CVE-2026-38532	A Broken Object-Level Authorization (BOLA) in the /Contact/Persons/PersonController.php endpoint of Webkul Krayin CRM v2.2.x allows authenticated attackers to arbitrarily read, modify, and permanently delete any contact owned by other users via supplying a crafted GET request.	8.1	More Details
CVE-2026-28291	simple-git enables running native Git commands from JavaScript. Versions up to and including 3.31.1 allow execution of arbitrary commands through Git option manipulation, bypassing safety checks meant to block dangerous options like -u and --upload-pack. The flaw stems from an incomplete fix for CVE-2022-25860, as Git's flexible option parsing allows numerous character combinations (e.g., -vu, -4u, -nu) to circumvent the regular-expression-based blocklist in the unsafe operations plugin. Due to the virtually infinite number of valid option variants that Git accepts, a complete blocklist-based mitigation may be infeasible without fully emulating Git's option parsing behavior. This issue has been fixed in version 3.32.0.	8.1	More Details
CVE-2026-35645	OpenClaw before 2026.3.25 contains a privilege escalation vulnerability in the gateway plugin subagent fallback deleteSession function that uses a synthetic operator.admin runtime scope. Attackers can exploit this by triggering session deletion without a request-scoped client to execute privileged operations with unintended administrative scope.	8.1	More Details
CVE-2026-5913	Out of bounds read in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Low)	8.1	More Details
CVE-2026-5907	Insufficient data validation in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory read via a crafted video file. (Chromium security severity: Low)	8.1	More Details
CVE-2026-40093	nimiq-blockchain provides persistent block storage for Nimiq's Rust implementation. In 1.3.0 and earlier, block timestamp validation enforces that timestamp >= parent.timestamp for non-skip blocks and timestamp == parent.timestamp + MIN_PRODUCER_TIMEOUT for skip blocks, but there is no visible upper bound check against the wall clock. A malicious block-producing validator can set block timestamps arbitrarily far in the future. This directly affects reward calculations via Policy::supply_at() and batch_delay() in blockchain/src/reward.rs, inflating the monetary supply beyond the intended emission schedule.	8.1	More Details
CVE-2026-39393	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.4.0, the install route guard in ci4ms relies solely on a volatile cache check (cache('settings')) combined with .env file existence to block post-installation access to the setup wizard. When the database is temporarily unreachable during a cache miss (TTL expiry or admin-triggered cache clear), the guard fails open, allowing an unauthenticated attacker to overwrite the .env file with attacker-controlled database credentials, achieving full application takeover. This vulnerability is fixed in 0.31.4.0.	8.1	More Details
CVE-2026-38530	A Broken Object-Level Authorization (BOLA) in the /Controllers/Lead/LeadController.php endpoint of Webkul Krayin CRM v2.2.x allows authenticated attackers to arbitrarily read, modify, and permanently delete any lead owned by other users via supplying a crafted GET request.	8.1	More Details
CVE-2026-5915	Insufficient validation of untrusted input in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Low)	8.1	More Details
CVE-2026-34512	OpenClaw before 2026.3.25 contains an improper access control vulnerability in the HTTP /sessions/:sessionKey/kill route that allows any bearer-authenticated user to invoke admin-level session termination functions without proper scope validation. Attackers can exploit this by sending authenticated requests to kill arbitrary subagent sessions via the killSubagentRunAdmin function, bypassing ownership and operator scope restrictions.	8.1	More Details

CVE-2026-40070	BSV Ruby SDK is the Ruby SDK for the BSV blockchain. From 0.3.1 to before 0.8.2, BSV::Wallet::WalletClient#acquire_certificate persists certificate records to storage without verifying the certifier's signature over the certificate contents. In acquisition_protocol: 'direct', the caller supplies all certificate fields (including signature:) and the record is written to storage verbatim. In acquisition_protocol: 'issuance', the client POSTs to a certifier URL and writes whatever signature the response body contains, also without verification. An attacker who can reach either API (or who controls a certifier endpoint targeted by the issuance path) can forge identity certificates that subsequently appear authentic to list_certificates and prove_certificate.	8.1	More Details
CVE-2026-25208	Integer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers.This issue affects Escargot: 97e8115ab1110bc502b4b5e4a0c689a71520d335.	8.1	More Details
CVE-2026-40393	In Mesa before 25.3.6 and 26 before 26.0.1, out-of-bounds memory access can occur in WebGPU because the amount of to-be-allocated data depends on an untrusted party, and is then used for alloca.	8.1	More Details
CVE-2026-33466	Improper Limitation of a Pathname to a Restricted Directory (CWE-22) in Logstash can lead to arbitrary file write and potentially remote code execution via Relative Path Traversal (CAPEC-139). The archive extraction utilities used by Logstash do not properly validate file paths within compressed archives. An attacker who can serve a specially crafted archive to Logstash through a compromised or attacker-controlled update endpoint can write arbitrary files to the host filesystem with the privileges of the Logstash process. In certain configurations where automatic pipeline reloading is enabled, this can be escalated to remote code execution.	8.1	More Details
CVE-2026-39394	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.4.0, the Install::index() controller reads the host POST parameter without any validation and passes it directly into updateEnvSettings(), which writes it into the .env file via preg_replace(). Because newline characters in the value are not stripped, an attacker can inject arbitrary configuration directives into the .env file. The install routes have CSRF protection explicitly disabled, and the InstallFilter can be bypassed when cache('settings') is empty (cache expiry or fresh deployment). This vulnerability is fixed in 0.31.4.0.	8.1	More Details
CVE-2026-35589	nanobot is a personal AI assistant. Versions prior to 0.1.5 contain a Cross-Site WebSocket Hijacking (CSWSH) vulnerability exists in the bridge's WebSocket server in bridge/src/server.ts, resulting from an incomplete remediation of CVE-2026-2577. The original fix changed the binding from 0.0.0.0 to 127.0.0.1 and added an optional BRIDGE_TOKEN parameter, but token authentication is disabled by default and the server does not validate the Origin header during the WebSocket handshake. Because browsers do not enforce the Same-Origin Policy on WebSockets unless the server explicitly denies cross-origin connections, any website visited by a user running the bridge can establish a WebSocket connection to ws://127.0.0.1:3001/ and gain full access to the bridge API. This allows an attacker to hijack the WhatsApp session, read incoming messages, steal authentication QR codes, and send messages on behalf of the user. This issue has bee fixed in version 0.1.5.	8.0	More Details
CVE-2026-33826	Improper input validation in Windows Active Directory allows an authorized attacker to execute code over an adjacent network.	8.0	More Details
CVE-2026-27912	Improper authorization in Windows Kerberos allows an authorized attacker to elevate privileges over an adjacent network.	8.0	More Details
CVE-2026-31281	Totara LMS v19.1.5 and before is vulnerable to HTLM Injection. An attacker can inject malicious HTLM code in a message and send it to all the users in the application, resulting in executing the code and may lead to session hijacking and executing commands on the victim's browser.	8.0	More Details
CVE-2026-30818	An OS command injection vulnerability in the dnsmasq module of TP-Link Archer AX53 v1.0 allows an authenticated adjacent attacker to execute arbitrary code when a specially crafted configuration file is processed due to insufficient input validation. Successful exploitation may allow the attacker to modify device configuration, access sensitive information, or further compromise system integrity. This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	8.0	More Details
CVE-2026-30815	An OS command injection vulnerability in the OpenVPN module of TP-Link Archer AX53 v1.0 allows an authenticated adjacent attacker to execute system commands when a specially crafted configuration file is processed due to insufficient input validation. Successful exploitation may allow modification of configuration files, disclosure of sensitive information, or further compromise of device integrity. This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	8.0	More Details
CVE-2026-30814	A stack-based buffer overflow in the tmpServer module of TP-Link Archer AX53 v1.0 allows an authenticated adjacent attacker to trigger a segmentation fault and potentially execute arbitrary code via a specially crafted configuration file. Successful exploitation may cause a crash and could allow arbitrary code execution, enabling modification of device state, exposure of sensitive data, or further compromise of device integrity. This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	8.0	More Details
CVE-2026-40149	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the gateway's /api/approval/allow-list endpoint permits unauthenticated modification of the tool approval allowlist when no auth_token is configured (the default). By adding dangerous tool names (e.g., shell_exec, file_write) to the allowlist, an attacker can cause the ExecApprovalManager to auto-approve all future agent invocations of those tools, bypassing the human-in-the-loop safety mechanism that the approval system is specifically designed to enforce. This vulnerability is fixed in 4.5.128.	7.9	More Details

CVE-2026-32189	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-35641	OpenClaw before 2026.3.24 contains an arbitrary code execution vulnerability in local plugin and hook installation that allows attackers to execute malicious code by crafting a .npmrc file with a git executable override. During npm install execution in the staged package directory, attackers can leverage git dependencies to trigger execution of arbitrary programs specified in the attacker-controlled .npmrc configuration file.	7.8	More Details
CVE-2026-27910	Improper handling of insufficient permissions or privileges in Windows Installer allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32159	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32160	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32184	Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32183	Improper neutralization of special elements used in a command ('command injection') in Windows Snipping Tool allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-32164	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-40156	PraisonAI is a multi-agent teams system. Prior to 4.5.128, PraisonAI automatically loads a file named tools.py from the current working directory to discover and register custom agent tools. This loading process uses importlib.util.spec_from_file_location and immediately executes module-level code via spec.loader.exec_module() without explicit user consent, validation, or sandboxing. The tools.py file is loaded implicitly, even when it is not referenced in configuration files or explicitly requested by the user. As a result, merely placing a file named tools.py in the working directory is sufficient to trigger code execution. This behavior violates the expected security boundary between user-controlled project files (e.g., YAML configurations) and executable code, as untrusted content in the working directory is treated as trusted and executed automatically. If an attacker can place a malicious tools.py file into a directory where a user or automated system (e.g., CI/CD pipeline) runs praisonai, arbitrary code execution occurs immediately upon startup, before any agent logic begins. This vulnerability is fixed in 4.5.128.	7.8	More Details
CVE-2026-32165	Use after free in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32168	Improper input validation in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27806	Fleet is open source device management software. Prior to 4.81.1, the Orbit agent's FileVault disk encryption key rotation flow on collects a local user's password via a GUI dialog and interpolates it directly into a Tcl/expect script executed via exec.Command("expect", "-c", script). Because the password is inserted into Tcl brace-quoted send {%s}, a password containing } terminates the literal and injects arbitrary Tcl commands. Since Orbit runs as root, this allows a local unprivileged user to escalate to root privileges. This vulnerability is fixed in 4.81.1.	7.8	More Details
CVE-2026-32163	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-40031	MemProcFS before 5.17 contains multiple unsafe library-loading patterns that enable DLL and shared-library hijacking across six attack surfaces, including bare-name LoadLibraryU and dlopen calls without path qualification for vmmpyc, libMSCompression, and plugin DLLs. An attacker who places a malicious DLL or shared library in the working directory or manipulates LD_LIBRARY_PATH can achieve arbitrary code execution when MemProcFS loads.	7.8	More Details
CVE-2026-32192	Deserialization of untrusted data in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32197	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in	7.8	More Details

34630	that a victim must open a malicious file.		
CVE-2026-27287	InCopy versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2026-35625	OpenClaw before 2026.3.25 contains a privilege escalation vulnerability where silent local shared-auth reconnects auto-approve scope-upgrade requests, widening paired device permissions from operator.read to operator.admin. Attackers can exploit this by triggering local reconnection to silently escalate privileges and achieve remote code execution on the node.	7.8	More Details
CVE-2026-33793	An Execution with Unnecessary Privileges vulnerability in the User Interface (UI) of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to gain root privileges, thus compromising the system. When a configuration that allows unsigned Python op scripts is present on the device, a non-root user is able to execute malicious op scripts as a root-equivalent user, leading to privilege escalation. This issue affects Junos OS: * All versions before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R1-S2, 24.2R2, * from 24.4 before 24.4R1-S2, 24.4R2; Junos OS Evolved: * All versions before 22.4R3-S7-EVO, * from 23.2 before 23.2R2-S4-EVO, * from 23.4 before 23.4R2-S6-EVO, * from 24.2 before 24.2R2-EVO, * from 24.4 before 24.4R1-S1-EVO, 24.4R2-EVO.	7.8	More Details
CVE-2026-33788	A Missing Authentication for Critical Function vulnerability in the Flexible PIC Concentrators (FPCs) of Juniper Networks Junos OS Evolved on PTX Series allows a local, authenticated attacker with low privileges to gain direct access to FPCs installed in the device. A local user with low privileges can gain direct access to the installed FPCs as a high privileged user, which can potentially lead to a full compromise of the affected component. This issue affects Junos OS Evolved on PTX10004, PTX10008, PTX100016, with JNP10K-LC1201 or JNP10K-LC1202: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-S3-EVO, * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO.	7.8	More Details
CVE-2026-34631	InCopy versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27292	Adobe Framemaker versions 2022.8 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-5726	ASDA-Soft Stack-based Buffer Overflow Vulnerability	7.8	More Details
CVE-2026-27293	Adobe Framemaker versions 2022.8 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27294	Adobe Framemaker versions 2022.8 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2026-27295	Adobe Framemaker versions 2022.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34734	HDF5 is software for managing data. In 1.14.1-2 and earlier, a heap-use-after-free was found in the h5dump helper utility. An attacker who can supply a malicious h5 file can trigger a heap use-after-free. The freed object is referenced in a memmove call from H5T__conv_struct. The original object was allocated by H5D__typeinfo_init_phase3 and freed by H5D__typeinfo_term.	7.8	More Details
CVE-2026-29923	The pstrip64.sys driver in EnTech Taiwan PowerStrip <=3.90.736 allows local users to escalate privileges to SYSTEM via a crafted IOCTL request enabling unprivileged users to map arbitrary physical memory into their address space and modify critical kernel structures.	7.8	More Details
CVE-2026-34971	Wasmtime is a runtime for WebAssembly. From 32.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime's Cranelift compilation backend contains a bug on aarch64 when performing a certain shape of heap accesses which means that the wrong address is accessed. When combined with explicit bounds checks a guest WebAssembly module this can create a situation where there are two diverging computations for the same address: one for the address to bounds-check and one for the address to load. This difference in address being operated on means that a guest module can pass a bounds check but then load a different address. Combined together this enables an arbitrary read/write primitive for guest WebAssembly when accesssing host memory. This is a sandbox escape as guests are able to read/write arbitrary host memory. This vulnerability has a few ingredients, all of which must be met, for this situation to occur and bypass the sandbox restrictions. This miscompiled shape of load only occurs on 64-bit WebAssembly linear memories, or when Config::wasm_memory64 is enabled. 32-bit WebAssembly is not affected. Spectre mitigations or signals-based-traps must be disabled. When spectre mitigations are enabled then the offending shape of load is not generated. When signals-based-traps are disabled then spectre mitigations are also automatically disabled. The specific bug in Cranelift is a miscompile of a load of the shape load(iadd(base, ishl(index, amt))) where amt is a constant. The amt value is masked incorrectly to test if it's a certain value, and this incorrect mask means	7.8	More Details

	that Cranelift can pattern-match this lowering rule during instruction selection erroneously, diverging from WebAssembly's and Cranelift's semantics. This incorrect lowering would, for example, load an address much further away than intended as the correct address's computation would have wrapped around to a smaller value insetad. This vulnerability is fixed in 36.0.7, 42.0.2, and 43.0.1.		
CVE-2026-27296	Adobe Framemaker versions 2022.8 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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-2026-27297	Adobe Framemaker versions 2022.8 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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-2026-27298	Adobe Framemaker versions 2022.8 and earlier are affected by an Access of Resource Using Incompatible Type ('Type Confusion') 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-2026-33023	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. In versions 1.8.7 and prior, when built with the --with-gdk-pixbuf2 option, a use-after-free vulnerability exists in load_with_gdkpixbuf() in loader.c. The cleanup path manually frees the sixel_frame_t object and its internal buffers without consulting the reference count, even though the object was created via the refcounted constructor sixel_frame_new() and exposed to the public callback. A callback that calls sixel_frame_ref(frame) to retain a logically valid reference will hold a dangling pointer after sixel_helper_load_image_file() returns, and any subsequent access to the frame or its fields triggers a use-after-free confirmed by AddressSanitizer. The root cause is a consistency failure between two cleanup strategies in the same codebase: sixel_frame_unref() is used in load_with_builtin() but raw free() is used in load_with_gdkpixbuf(). An attacker supplying a crafted image to any application built against libsixel with gdk-pixbuf2 support can trigger this reliably, potentially leading to information disclosure, memory corruption, or code execution. This issue has been fixed in version 1.8.7-r1.	7.8	More Details
CVE-2026-39853	osslsigncode is a tool that implements Authenticode signing and timestamping. Prior to 2.12, A stack buffer overflow vulnerability exists in osslsigncode in several signature verification paths. During verification of a PKCS#7 signature, the code copies the digest value from a parsed SpcIndirectDataContent structure into a fixed-size stack buffer (mdbuf[EVP_MAX_MD_SIZE], 64 bytes) without validating that the source length fits within the destination buffer. This pattern is present in the verification handlers for PE, MSI, CAB, and script files. An attacker can craft a malicious signed file with an oversized digest field in SpcIndirectDataContent. When a user verifies such a file with osslsigncode verify, the unbounded memcpy can overflow the stack buffer and corrupt adjacent stack state. This vulnerability is fixed in 2.12.	7.8	More Details
CVE-2026-34618	Illustrator versions 30.2, 29.8.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27313	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27312	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-32222	Untrusted pointer dereference in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32198	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-32199	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-32200	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-25203	Samsung MagicINFO 9 Server Incorrect Default Permissions Local Privilege Escalation Vulnerability This issue affects MagicINFO 9 Server: less than 21.1091.1.	7.8	More Details
CVE-2026-40029	parseusbs before 1.9 contains an OS command injection vulnerability in parseUSBs.py where LNK file paths are passed unsanitized into an os.popen() shell command, allowing arbitrary command execution via crafted .lnk filenames containing shell metacharacters. An attacker can craft a .lnk filename with embedded shell metacharacters that execute arbitrary commands on the forensic examiner's machine during USB artifact parsing.	7.8	More Details
CVE-	parseusbs before 1.9 contains an OS command injection vulnerability where the volume listing path argument (-v		

2026-40030	flag) is passed unsanitized into an os.popen() shell command with ls, allowing arbitrary command injection via crafted volume path arguments containing shell metacharacters. An attacker can provide a crafted volume path via the -v flag that injects arbitrary commands during volume content enumeration.	7.8	More Details
CVE-2026-32155	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-40032	UAC (Unix-like Artifacts Collector) before 3.3.0-rc1 contains a command injection vulnerability in the placeholder substitution and command execution pipeline where the _run_command() function passes constructed command strings directly to eval without proper sanitization. Attackers can inject shell metacharacters or command substitutions through attacker-controlled inputs including %line% values from foreach iterators and %user% / %user_home% values derived from system files to achieve arbitrary command execution with the privileges of the UAC process.	7.8	More Details
CVE-2026-33095	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-27311	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-33098	Use after free in Windows Container Isolation FS Filter Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-33101	Use after free in Windows Print Spooler Components allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-33825	Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-34627	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34628	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-34629	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27289	Photoshop Desktop versions 27.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2026-27310	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-32158	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27911	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32076	Out-of-bounds read in Windows Storage Spaces Controller allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27291	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-26179	Double free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-	Untrusted pointer dereference in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker	7.8	More

27919	to elevate privileges locally.		Details
CVE-2026-26153	Out-of-bounds read in Windows Encrypting File System (EFS) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27918	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Shell allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32090	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Speech Brokered Api allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27916	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26176	Heap-based buffer overflow in Windows Client Side Caching driver (csc.sys) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27238	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27283	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-27284	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2026-26172	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27915	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26180	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26170	Improper input validation in Microsoft PowerShell allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26168	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27914	Improper access control in Microsoft Management Console allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26163	Double free in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26162	Access of resource using incompatible type ('type confusion') in Windows OLE allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26161	Untrusted pointer dereference in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26160	Missing authentication for critical function in Windows Remote Desktop Licensing Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26159	Missing authentication for critical function in Windows Remote Desktop Licensing Service allows an authorized attacker to elevate privileges locally.	7.8	More Details

CVE-2026-26156	Heap-based buffer overflow in Windows Hyper-V allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-20930	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-23657	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2026-27920	Untrusted pointer dereference in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26143	Improper input validation in Microsoft PowerShell allows an unauthorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-26184	Buffer over-read in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-28261	Dell Elastic Cloud Storage, version 3.8.1.7 and prior, and Dell ObjectScale, versions prior to 4.1.0.3 and version 4.2.0.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to secret exposure. The attacker may be able to use the exposed secret to access the vulnerable system with privileges of the compromised account.	7.8	More Details
CVE-2026-27907	Integer underflow (wrap or wraparound) in Windows Storage Spaces Controller allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27923	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32152	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27927	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32069	Double free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32074	Double free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32077	Untrusted pointer dereference in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32078	Use after free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32153	Use after free in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26183	Improper access control in Windows RPC API allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27909	Use after free in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-32154	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details

CVE-2026-32089	Use after free in Windows Speech Brokered Api allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-26181	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-27924	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-35446	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 24.0.0 to before 27.0.3 and 28.0.1, an incorrect order of operations in the FilesDownloadHandler could result in an attacker escaping the intended download directories. This vulnerability is fixed in 27.0.3 and 28.0.1.	7.7	More Details
CVE-2026-34619	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access unauthorized files or directories outside the intended restrictions. Exploitation of this issue does not require user interaction.	7.7	More Details
CVE-2026-40683	In OpenStack Keystone before 28.0.1, the LDAP identity backend does not convert the user enabled attribute to a boolean when the user_enabled_invert configuration option is False (the default). The _ldap_res_to_model method in the UserApi class only performed string-to-boolean conversion when user_enabled_invert was True. When False, the raw string value from LDAP (e.g., "FALSE") was used directly. Since non-empty strings are truthy in Python, users marked as disabled in LDAP were treated as enabled by Keystone, allowing them to authenticate and perform actions. All deployments using the LDAP identity backend without user_enabled_invert=True or user_enabled_emulation are affected.	7.7	More Details
CVE-2026-27913	Improper input validation in Windows BitLocker allows an unauthorized attacker to bypass a security feature locally.	7.7	More Details
CVE-2026-39843	Plane is an an open-source project management tool. From 0.28.0 to before 1.3.0, the remediation of GHSA-jcc6-f9v6-f7jw is incomplete which could lead to the same full read Server-Side Request Forgery when a normal html page contains a link tag with an href that redirects to a private IP address is supplied to Add link by an authenticated attacker with low privileges. Redirects for the main page URL are validated, but not the favicon fetch path. fetch_and_encode_favicon() still uses requests.get(favicon_url, ...) with the default redirect-following. This vulnerability is fixed in 1.3.0.	7.7	More Details
CVE-2026-32252	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 4.9.0, a cross-tenant authorization bypass exists in Chartbrew in GET /team/:team_id/template/generate/:project_id. The GET handler calls checkAccess(req, "updateAny", "chart") without awaiting the returned promise, and it does not verify that the supplied project_id belongs to req.params.team_id or to the caller's team. As a result, an authenticated attacker with valid template-generation permissions in their own team can request the template model for a project belonging to another team and receive victim project data. This vulnerability is fixed in 4.9.0.	7.7	More Details
CVE-2026-34853	Permission bypass vulnerability in the LBS module. Impact: Successful exploitation of this vulnerability may affect availability.	7.7	More Details
CVE-2026-40188	goshs is a SimpleHTTPServer written in Go. From 1.0.7 to before 2.0.0-beta.4, the SFTP command rename sanitizes only the source path and not the destination, so it is possible to write outside of the root directory of the SFTP. This vulnerability is fixed in 2.0.0-beta.4.	7.7	More Details
CVE-2026-40150	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, the web_crawl() function in praisonaiagents/tools/web_crawl_tools.py accepts arbitrary URLs from AI agents with zero validation. No scheme allowlisting, hostname/IP blocklisting, or private network checks are applied before fetching. This allows an attacker (or prompt injection in crawled content) to force the agent to fetch cloud metadata endpoints, internal services, or local files via file:// URLs. This vulnerability is fixed in 1.5.128.	7.7	More Details
CVE-2026-35668	OpenClaw before 2026.3.24 contains a path traversal vulnerability in sandbox enforcement allowing sandboxed agents to read arbitrary files from other agents' workspaces via unnormalized mediaUrl or fileUrl parameter keys. Attackers can exploit incomplete parameter validation in normalizeSandboxMediaParams and missing mediaLocalRoots context to access sensitive files including API keys and configuration data outside designated sandbox roots.	7.7	More Details
CVE-2026-31941	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, Chamilo LMS contains a Server-Side Request Forgery (SSRF) vulnerability in the Social Wall feature. The endpoint read_url_with_open_graph accepts a URL from the user via the social_wall_new_msg_main POST parameter and performs two server-side HTTP requests to that URL without validating whether the target is an internal or external resource. This allows an authenticated attacker to force the server to make arbitrary HTTP requests to internal services, scan internal ports, and access cloud instance metadata. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.7	More Details
CVE-	Execution with Unnecessary Privileges (CWE-250) in Kibana’s Fleet plugin debug route handlers can lead reading		

2026-4498	index data beyond their direct Elasticsearch RBAC scope via Privilege Abuse (CAPEC-122). This requires an authenticated Kibana user with Fleet sub-feature privileges (such as agents, agent policies, and settings management).	7.7	More Details
CVE-2026-33461	Incorrect Authorization (CWE-863) in Kibana can lead to information disclosure via Privilege Abuse (CAPEC-122). A user with limited Fleet privileges can exploit an internal API endpoint to retrieve sensitive configuration data, including private keys and authentication tokens, that should only be accessible to users with higher-level settings privileges. The endpoint composes its response by fetching full configuration objects and returning them directly, bypassing the authorization checks enforced by the dedicated settings APIs.	7.7	More Details
CVE-2026-39497	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 FOX woocommerce-currency-switcher allows Blind SQL Injection.This issue affects FOX: from n/a through <= 1.4.5.	7.6	More Details
CVE-2026-39466	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPMU DEV - Your All-in-One WordPress Platform Broken Link Checker broken-link-checker allows Blind SQL Injection.This issue affects Broken Link Checker: from n/a through <= 2.4.7.	7.6	More Details
CVE-2026-39487	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ameliabooking Amelia ameliabooking allows Blind SQL Injection.This issue affects Amelia: from n/a through <= 2.1.1.	7.6	More Details
CVE-2026-39479	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Brainstorm Force OttoKit suretriggers allows Blind SQL Injection.This issue affects OttoKit: from n/a through <= 1.1.20.	7.6	More Details
CVE-2026-39496	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in YayCommerce YayMail yaymail allows Blind SQL Injection.This issue affects YayMail: from n/a through <= 4.3.3.	7.6	More Details
CVE-2026-5301	Stored XSS in log viewer in CoolerControl/coolercontrol-ui <4.0.0 allows unauthenticated attackers to take over the service via malicious JavaScript in poisoned log entries	7.6	More Details
CVE-2026-33790	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an attacker sending a specific, malformed ICMPv6 packet to cause the srxpfe process to crash and restart. Continued receipt and processing of these packets will repeatedly crash the srxpfe process and sustain the Denial of Service (DoS) condition. During NAT64 translation, receipt of a specific, malformed ICMPv6 packet destined to the device will cause the srxpfe process to crash and restart. This issue cannot be triggered using IPv4 nor other IPv6 traffic. This issue affects Junos OS on SRX Series: * all versions before 21.2R3-S10, * all versions of 21.3, * from 21.4 before 21.4R3-S12, * all versions of 22.1, * from 22.2 before 22.2R3-S8, * all versions of 22.4, * from 22.4 before 22.4R3-S9, * from 23.2 before 23.2R2-S6, * from 23.4 before 23.4R2-S7, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2-S3, * from 25.2 before 25.2R1-S2, 25.2R2.	7.5	More Details
CVE-2026-33778	An Improper Validation of Syntactic Correctness of Input vulnerability in the IPsec library used by kmd and iked of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a complete Denial-of-Service (DoS). If an affected device receives a specifically malformed first ISAKMP packet from the initiator, the kmd/iked process will crash and restart, which momentarily prevents new security associations (SAs) for from being established. Repeated exploitation of this vulnerability causes a complete inability to establish new VPN connections. This issue affects Junos OS on SRX Series and MX Series: * all versions before 22.4R3-S9, * 23.2 version before 23.2R2-S6, * 23.4 version before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R1-S2, 25.2R2.	7.5	More Details
CVE-2026-40164	jq is a command-line JSON processor. Before commit 0c7d133c3c7e37c00b6d46b658a02244fdd3c784, jq used MurmurHash3 with a hardcoded, publicly visible seed (0x432A9843) for all JSON object hash table operations, which allowed an attacker to precompute key collisions offline. By supplying a crafted JSON object (~100 KB) where all keys hashed to the same bucket, hash table lookups degraded from O(1) to O(n), turning any jq expression into an O(n²) operation and causing significant CPU exhaustion. This affected common jq use cases such as CI/CD pipelines, web services, and data processing scripts, and was far more practical to exploit than existing heap overflow issues since it required only a small payload. This issue has been patched in commit 0c7d133c3c7e37c00b6d46b658a02244fdd3c784.	7.5	More Details
CVE-2026-33096	Out-of-bounds read in Windows HTTP.sys allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-33908	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below both 7.1.2-19 and 6.9.13-44, Magick frees the memory of the XML tree via the `DestroyXMLTree()` function; however, this process is executed recursively with no depth limit imposed. When Magick processes an XML file with deeply nested structures, it will exhaust the stack memory, resulting in a Denial of Service (DoS) attack. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	7.5	More Details
CVE-2026-22566	An Improper Access Control vulnerability could allow a malicious actor with access to the UniFi Play network to obtain UniFi Play WiFi credentials. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later	7.5	More Details

CVE-2026-40046	Integer Overflow or Wraparound vulnerability in Apache ActiveMQ, Apache ActiveMQ All, Apache ActiveMQ MQTT. The fix for "CVE-2025-66168: MQTT control packet remaining length field is not properly validated" was only applied to 5.19.2 (and future 5.19.x) releases but was missed for all 6.0.0+ versions. This issue affects Apache ActiveMQ: from 6.0.0 before 6.2.4; Apache ActiveMQ All: from 6.0.0 before 6.2.4; Apache ActiveMQ MQTT: from 6.0.0 before 6.2.4. Users are recommended to upgrade to version 6.2.4 or a 5.19.x version starting with 5.19.2 or later (currently latest is 5.19.5), which fixes the issue.	7.5	More Details
CVE-2026-39611	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in kutethemes KuteShop kuteshop allows PHP Local File Inclusion.This issue affects KuteShop: from n/a through <= 4.2.9.	7.5	More Details
CVE-2026-40036	Unfurl before 2026.04 contains an unbounded zlib decompression vulnerability in parse_compressed.py that allows remote attackers to cause denial of service. Attackers can submit highly compressed payloads via URL parameters to the /json/visjs endpoint that expand to gigabytes, exhausting server memory and crashing the service.	7.5	More Details
CVE-2026-22565	An Improper Input Validation vulnerability could allow a malicious actor with access to the UniFi Play network to cause the device to stop responding. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later	7.5	More Details
CVE-2026-33901	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below both 7.1.2-19 and 6.9.13-44, a heap buffer overflow occurs in the MVG decoder that could result in an out of bounds write when processing a crafted image. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	7.5	More Details
CVE-2026-34020	Use of GET Request Method With Sensitive Query Strings vulnerability in Apache OpenMeetings. The REST login endpoint uses HTTP GET method with username and password passed as query parameters. Please check references regarding possible impact This issue affects Apache OpenMeetings: from 3.1.3 before 9.0.0. Users are recommended to upgrade to version 9.0.0, which fixes the issue.	7.5	More Details
CVE-2026-32605	nimiq/core-rs-albatross is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.3.0, an untrusted peer could crash a validator by publishing a signed tendermint proposal message where signer == validators.num_validators(). ProposalSender::send uses > instead of >= for the signer bounds check, so the equality case passes and reaches validators.get_validator_by_slot_band(signer), which panics with an out-of-bounds index before any signature verification runs. This issue has been fixed in version 1.3.0.	7.5	More Details
CVE-2026-33266	Use of Hard-coded Cryptographic Key vulnerability in Apache OpenMeetings. The remember-me cookie encryption key is set to default value in openmeetings.properties and not being auto-rotated. In case OM admin hasn't changed the default encryption key, an attacker who has stolen a cookie from a logged-in user can get full user credentials. This issue affects Apache OpenMeetings: from 6.1.0 before 9.0.0. Users are recommended to upgrade to version 9.0.0, which fixes the issue.	7.5	More Details
CVE-2026-32203	Stack-based buffer overflow in .NET and Visual Studio allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-5440	A memory exhaustion vulnerability exists in the HTTP server due to unbounded use of the `Content-Length` header. The server allocates memory directly based on the attacker supplied header value without enforcing an upper limit. A crafted HTTP request containing an extremely large `Content-Length` value can trigger excessive memory allocation and server termination, even without sending a request body.	7.5	More Details
CVE-2026-3360	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to an Insecure Direct Object Reference in all versions up to, and including, 3.9.7. This is due to missing authentication and authorization checks in the `pay_incomplete_order()` function. The function accepts an attacker-controlled `order_id` parameter and uses it to look up order data, then writes billing fields to the order owner's profile (`$order_data->user_id`) without verifying the requester's identity or ownership. Because the Tutor nonce (`_tutor_nonce`) is exposed on public frontend pages, this makes it possible for unauthenticated attackers to overwrite the billing profile (name, email, phone, address) of any user who has an incomplete manual order, by sending a crafted POST request with a guessed or enumerated `order_id`.	7.5	More Details
CVE-2026-39677	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Creatives_Planet Emphires emphires allows PHP Local File Inclusion.This issue affects Emphires: from n/a through <= 3.9.	7.5	More Details
CVE-2026-5439	A memory exhaustion vulnerability exists in ZIP archive processing. Orthanc automatically extracts ZIP archives uploaded to certain endpoints and trusts metadata fields describing the uncompressed size of archived files. An attacker can craft a small ZIP archive containing a forged size value, causing the server to allocate extremely large buffers during extraction.	7.5	More Details
CVE-2026-39679	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ApusTheme Freeio freeio allows PHP Local File Inclusion.This issue affects Freeio: from n/a through <= 1.3.21.	7.5	More Details
CVE-2026-39681	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ApusTheme Homeo homeo allows PHP Local File Inclusion.This issue affects Homeo: from n/a through <= 1.2.59.	7.5	More Details

CVE-2026-5438	A gzip decompression bomb vulnerability exists when Orthanc processes HTTP request with `Content-Encoding: gzip`. The server does not enforce limits on decompressed size and allocates memory based on attacker-controlled compression metadata. A specially crafted gzip payload can trigger excessive memory allocation and exhaust system memory.	7.5	More Details
CVE-2026-39889	PraisonAI is a multi-agent teams system. Prior to 4.5.115, the A2U (Agent-to-User) event stream server in PraisonAI exposes all agent activity without authentication. The create_a2u_routes() function registers the following endpoints with NO authentication checks: /a2u/info, /a2u/subscribe, /a2u/events/{stream_name}, /a2u/events/sub/{id}, and /a2u/health. This vulnerability is fixed in 4.5.115.	7.5	More Details
CVE-2025-62188	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Apache DolphinScheduler. This vulnerability may allow unauthorized actors to access sensitive information, including database credentials. This issue affects Apache DolphinScheduler versions 3.1.*. Users are recommended to upgrade to: * version ≥ 3.2.0 if using 3.1.x As a temporary workaround, users who cannot upgrade immediately may restrict the exposed management endpoints by setting the following environment variable: ``` MANAGEMENT_ENDPOINTS_WEB_EXPOSURE_INCLUDE=health,metrics,prometheus ``` Alternatively, add the following configuration to the application.yaml file: ``` management: endpoints: web: exposure: include: health,metrics,prometheus ``` This issue has been reported as CVE-2023-48796: https://cveprocess.apache.org/cve5/CVE-2023-48796	7.5	More Details
CVE-2026-39885	FrontMCP is a TypeScript-first framework for the Model Context Protocol (MCP). Prior to 2.3.0, the mcp-from-openapi library uses @apidevtools/json-schema-ref-parser to dereference $ref pointers in OpenAPI specifications without configuring any URL restrictions or custom resolvers. A malicious OpenAPI specification containing $ref values pointing to internal network addresses, cloud metadata endpoints, or local files will cause the library to fetch those resources during the initialize() call. This enables Server-Side Request Forgery (SSRF) and local file read attacks when processing untrusted OpenAPI specifications. This vulnerability is fixed in 2.3.0.	7.5	More Details
CVE-2026-5437	An out-of-bounds read vulnerability exists in `DicomStreamReader` during DICOM meta-header parsing. When processing malformed metadata structures, the parser may read beyond the bounds of the allocated metadata buffer. Although this issue does not typically crash the server or expose data directly to the attacker, it reflects insufficient input validation in the parsing logic.	7.5	More Details
CVE-2026-22750	When configuring SSL bundles in Spring Cloud Gateway by using the configuration property spring.ssl.bundle, the configuration was silently ignored and the default SSL configuration was used instead. Note: The 4.2.x branch is no longer under open source support. If you are using Spring Cloud Gateway 4.2.0 and are not an enterprise customer, you can upgrade to any Spring Cloud Gateway 4.2.x release newer than 4.2.0 available on Maven Centeral https://repo1.maven.org/maven2/org/springframework/cloud/spring-cloud-gateway/ . Ideally if you are not an enterprise customer, you should be upgrading to 5.0.2 or 5.1.1 which are the current supported open source releases.	7.5	More Details
CVE-2026-1584	A flaw was found in gnutls. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted ClientHello message with an invalid Pre-Shared Key (PSK) binder value during the TLS handshake. This can lead to a NULL pointer dereference, causing the server to crash and resulting in a remote Denial of Service (DoS) condition.	7.5	More Details
CVE-2026-4352	The JetEngine plugin for WordPress is vulnerable to SQL Injection via the Custom Content Type (CCT) REST API search endpoint in all versions up to, and including, 3.8.6.1. This is due to the `_cct_search` parameter being interpolated directly into a SQL query string via `sprintf()` without sanitization or use of `$wpdb->prepare()`. WordPress REST API's `wp_unslash()` call on `$_GET` strips the `wp_magic_quotes()` protection, allowing single-quote-based injection. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The Custom Content Types module must be enabled with at least one CCT configured with a public REST GET endpoint for exploitation.	7.5	More Details
CVE-2026-33116	Loop with unreachable exit condition ('infinite loop') in .NET, .NET Framework, Visual Studio allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-34483	Improper Encoding or Escaping of Output vulnerability in the JsonAccessLogValve component of Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.20, from 10.1.0-M1 through 10.1.53, from 9.0.40 through 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117 , which fix the issue.	7.5	More Details
CVE-2026-23666	Concurrent execution using shared resource with improper synchronization ('race condition') in .NET Framework allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-27282	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue requires user interaction.	7.5	More Details
CVE-2026-39684	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in UnTheme OrganicFood organicfood allows PHP Local File Inclusion.This issue affects OrganicFood: from n/a through <= 3.6.4.	7.5	More Details
CVE-2026-33810	When verifying a certificate chain containing excluded DNS constraints, these constraints are not correctly applied to wildcard DNS SANs which use a different case than the constraint. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.	7.5	More Details

CVE-2026-26171	Uncontrolled resource consumption in .NET allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2025-12664	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.0 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an unauthenticated user to cause denial of service by sending repeated GraphQL queries.	7.5	More Details
CVE-2026-1092	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.10 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an unauthenticated user to cause denial of service due to improper input validation of JSON payloads.	7.5	More Details
CVE-2026-40116	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the /media-stream WebSocket endpoint in PraisonAI's call module accepts connections from any client without authentication or Twilio signature validation. Each connection opens an authenticated session to OpenAI's Realtime API using the server's API key. There are no limits on concurrent connections, message rate, or message size, allowing an unauthenticated attacker to exhaust server resources and drain the victim's OpenAI API credits. This vulnerability is fixed in 4.5.128.	7.5	More Details
CVE-2026-39623	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in kutethemes Biolife biolife allows PHP Local File Inclusion.This issue affects Biolife: from n/a through <= 3.2.3.	7.5	More Details
CVE-2026-34487	Insertion of Sensitive Information into Log File vulnerability in the cloud membership for clustering component of Apache Tomcat exposed the Kubernetes bearer token. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.20, from 10.1.0-M1 through 10.1.53, from 9.0.13 through 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fix the issue.	7.5	More Details
CVE-2026-34486	Missing Encryption of Sensitive Data vulnerability in Apache Tomcat due to the fix for CVE-2026-29146 allowing the bypass of the EncryptInterceptor. This issue affects Apache Tomcat: 11.0.20, 10.1.53, 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fix the issue.	7.5	More Details
CVE-2026-29146	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.0.0-M1 through 10.1.52, from 9.0.13 through 9..115, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Users are recommended to upgrade to version 11.0.19, 10.1.53 and 9.0.116, which fixes the issue.	7.5	More Details
CVE-2026-5747	An out-of-bounds write issue in the virtio PCI transport in Amazon Firecracker 1.13.0 through 1.14.3 and 1.15.0 on x86_64 and aarch64 might allow a local guest user with root privileges to crash the Firecracker VMM process or potentially execute arbitrary code on the host via modification of virtio queue configuration registers after device activation. Achieving code execution on the host requires additional preconditions, such as the use of a custom guest kernel or specific snapshot configurations. To remediate this, users should upgrade to Firecracker 1.14.4 or 1.15.1 and later.	7.5	More Details
CVE-2026-29129	Configured cipher preference order not preserved vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.16 through 11.0.18, from 10.1.51 through 10.1.52, from 9.0.114 through 9.0.115. Users are recommended to upgrade to version 11.0.20, 10.1.53 or 9.0.116, which fix the issue.	7.5	More Details
CVE-2026-24880	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache Tomcat via invalid chunk extension. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.1.0-M1 through 10.1.52, from 9.0.0.M1 through 9.0.115, from 8.5.0 through 8.5.100, from 7.0.0 through 7.0.109. Other, unsupported versions may also be affected. Users are recommended to upgrade to version 11.0.20, 10.1.52 or 9.0.116, which fix the issue.	7.5	More Details
CVE-2026-35186	Wasmtime is a runtime for WebAssembly. From 25.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime's Winch compiler backend contains a bug where translating the table.grow operator causes the result to be incorrectly typed. For 32-bit tables this means that the result of the operator, internally in Winch, is tagged as a 64-bit value instead of a 32-bit value. This invalid internal representation of Winch's compiler state compounds into further issues depending on how the value is consumed. The primary consequence of this bug is that bytes in the host's address space can be stored/read from. This is only applicable to the 16 bytes before linear memory, however, as the only significant return value of table.grow that can be misinterpreted is -1. The bytes before linear memory are, by default, unmapped memory. Wasmtime will detect this fault and abort the process, however, because wasm should not be able to access these bytes. Overall this this bug in Winch represents a DoS vector by crashing the host process, a correctness issue within Winch, and a possible leak of up to 16-bytes before linear memory. Wasmtime's default compiler is Cranelift, not Winch, and Wasmtime's default settings are to place guard pages before linear memory. This means that Wasmtime's default configuration is not affected by this issue, and when explicitly choosing Winch Wasmtime's otherwise default configuration leads to a DoS. Disabling guard pages before linear memory is required to possibly leak up to 16-bytes of host data. This vulnerability is fixed in 36.0.7, 42.0.2, and 43.0.1.	7.5	More Details
CVE-2026-32283	If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.	7.5	More Details
CVE-2026-23708	A improper authentication vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5.0 through 7.5.2 may allow an unauthenticated attacker to bypass authentication via replaying captured 2FA request. The attack requires being able to intercept and decrypt authentication traffic and precise timing to replay the request before token expiration, which	7.5	More Details

	raises the attack complexity.		
CVE-2026-31923	Cleartext Transmission of Sensitive Information vulnerability in Apache APISIX. This can occur due to `ssl_verify` in openid-connect plugin configuration being set to false by default. This issue affects Apache APISIX: from 0.7 through 3.15.0. Users are recommended to upgrade to version 3.16.0, which fixes the issue.	7.5	More Details
CVE-2026-32281	Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.	7.5	More Details
CVE-2026-4338	The ActivityPub WordPress plugin before 8.0.2 does not properly filter posts to be displayed, allowed unauthenticated users to access drafts/scheduled/pending posts	7.5	More Details
CVE-2026-40069	BSV Ruby SDK is the Ruby SDK for the BSV blockchain. From 0.1.0 to before 0.8.2, BSV::Network::ARC's failure detection only recognises REJECTED and DOUBLE_SPEND_ATTEMPTED. ARC responses with txStatus values of INVALID, MALFORMED, MINED_IN_STALE_BLOCK, or any ORPHAN-containing extraInfo / txStatus are silently treated as successful broadcasts. Applications that gate actions on broadcaster success are tricked into trusting transactions that were never accepted by the network. This vulnerability is fixed in 0.8.2.	7.5	More Details
CVE-2026-32280	During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.	7.5	More Details
CVE-2026-39613	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in kutethemes Boutique kute-boutique allows PHP Local File Inclusion.This issue affects Boutique: from n/a through <= 2.3.3.	7.5	More Details
CVE-2026-26154	Improper input validation in Windows Server Update Service allows an unauthorized attacker to perform tampering over a network.	7.5	More Details
CVE-2026-32071	Null pointer dereference in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2025-50661	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of multiple parameters in the /url_rule.asp endpoint. An attacker can exploit this vulnerability by sending a crafted HTTP GET request with parameters name, en, ips, u, time, act, rpri, and log.	7.5	More Details
CVE-2025-50650	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to inadequate validation of input size in the routes_static parameter in the /router.asp endpoint.	7.5	More Details
CVE-2025-50653	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the name and mem parameters in the /time_group.asp endpoint.	7.5	More Details
CVE-2025-50654	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper validation of the id parameter in the /thd_member.asp endpoint.	7.5	More Details
CVE-2025-50655	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the name parameter in the /thd_group.asp endpoint.	7.5	More Details
CVE-2025-50657	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the pid parameter in the /trace.asp endpoint.	7.5	More Details
CVE-2025-50659	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the custom_error parameter in the /user.asp endpoint.	7.5	More Details
CVE-2025-50660	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the name parameter in the /url_member.asp endpoint.	7.5	More Details
CVE-2025-50662	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the name parameter in the /url_group.asp endpoint.	7.5	More Details
CVE-2025-50663	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the name parameter in the /usb_paswd.asp endpoint.	7.5	More Details
CVE-2025-	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of parameters in the /user_group.asp endpoint. The attacker can exploit this vulnerability by sending a crafted HTTP GET request with	7.5	More

50664	parameters name, mem, pri, and attr.		Details
CVE-2025-50665	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of input parameters in the /web_keyword.asp endpoint. An attacker can exploit this vulnerability by sending a crafted HTTP GET request via the name, en, time, mem_gb2312, and mem_utf8 parameters.	7.5	More Details
CVE-2025-50666	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of multiple parameters in the /web_post.asp endpoint. An attacker can exploit this vulnerability by sending a crafted HTTP GET request in parameters such as name, en, user_id, log, and time.	7.5	More Details
CVE-2025-50667	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the iface parameter in the /wan_line_detection.asp endpoint.	7.5	More Details
CVE-2025-50668	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the s parameter in the /web_list_opt.asp endpoint.	7.5	More Details
CVE-2025-50669	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 and DI-8003G 19.12.10A1 due to improper handling of the wan_ping parameter in the /wan_ping.asp endpoint.	7.5	More Details
CVE-2025-50670	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of parameters in the /xwgl_bwr.asp endpoint. An attacker can exploit this vulnerability by sending a crafted HTTP GET request in the name, qq, and time parameters.	7.5	More Details
CVE-2025-50671	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of parameters in the /xwgl_ref.asp endpoint. An attacker can exploit this vulnerability by sending a crafted HTTP GET request with excessively long strings in parameters name, en, user_id, shibie_name, time, act, log, and rpri.	7.5	More Details
CVE-2025-50672	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of parameters in the /yyxz_dlink.asp endpoint.	7.5	More Details
CVE-2026-32931	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an unrestricted file upload vulnerability in the exercise sound upload function allows an authenticated teacher to upload a PHP webshell by spoofing the Content-Type header to audio/mpeg. The uploaded file retains its original .php extension and is placed in a web-accessible directory, enabling Remote Code Execution as the web server user (www-data). This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.5	More Details
CVE-2026-31940	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, in main/lp/aicc_hacp.php, user-controlled request parameters are directly used to set the PHP session ID before loading global bootstrap. This leads to session fixation. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.5	More Details
CVE-2025-50652	An issue in D-Link DI-8003 16.07.26A1 related to improper handling of the id parameter in the /saveparm_usb.asp endpoint.	7.5	More Details
CVE-2025-50649	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper input validation in the vlan_name parameter in the /shut_set.asp endpoint.	7.5	More Details
CVE-2026-33350	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. Prior to 27.0.3 and 28.0.1, a SQL injection has been identified in some code sections for the MRI feedback popup window of the imaging browser. Attackers can use SQL ingestion to access/alter data on the server. This vulnerability is fixed in 27.0.3 and 28.0.1.	7.5	More Details
CVE-2025-50648	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to inadequate input validation in the /tggl.asp endpoint.	7.5	More Details
CVE-2019-25706	Across DR-810 contains an unauthenticated file disclosure vulnerability that allows remote attackers to download the rom-0 backup file containing sensitive information by sending a simple GET request. Attackers can access the rom-0 endpoint without authentication to retrieve and decompress the backup file, exposing router passwords and other sensitive configuration data.	7.5	More Details
CVE-2026-3396	WCAPF – WooCommerce Ajax Product Filter plugin is vulnerable to time-based SQL Injection via the 'post-author' parameter in all versions up to, and including, 4.2.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-4660	HashiCorp's go-getter library up to v1.8.5 may allow arbitrary file reads on the file system during certain git operations through a maliciously crafted URL. This vulnerability, CVE-2026-4660, is fixed in go-getter v1.8.6. This vulnerability does not affect the go-getter/v2 branch and package.	7.5	More Details
CVE-	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.12, a path		

2026-39408	traversal issue in toSSG() allows files to be written outside the configured output directory during static site generation. When using dynamic route parameters via ssgParams, specially crafted values can cause generated file paths to escape the intended output directory. This vulnerability is fixed in 4.12.12.	7.5	More Details
CVE-2026-39538	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Mikado Core mikado-core allows PHP Local File Inclusion.This issue affects Mikado Core: from n/a through <= 1.6.	7.5	More Details
CVE-2026-30075	OpenAirInterface Version 2.2.0 has a Buffer Overflow vulnerability in processing UplinkNASTransport containing Authentication Response containing a NAS PDU with oversize response (For example 100 byte). The response is decoded by AMF and passed to the AUSF component for verification. AUSF crashes on receiving this oversize response. This can prohibit users from further registration and verification and can cause Denial of Services (DoS).	7.5	More Details
CVE-2026-30080	OpenAirInterface v2.2.0 accepts Security Mode Complete without any integrity protection. Configuration has supported integrity NIA1 and NIA2. But if an UE sends initial registration request with only security capability IA0, OpenAirInterface accepts and proceeds. This downgrade security context can lead to the possibility of replay attack.	7.5	More Details
CVE-2026-40198	Net::CIDR::Lite versions before 0.23 for Perl does not validate IPv6 group count, which may allow IP ACL bypass. _pack_ipv6() does not check that uncompressed IPv6 addresses (without ::) have exactly 8 hex groups. Inputs like "abcd", "1:2:3", or "1:2:3:4:5:6:7" are accepted and produce packed values of wrong length (3, 7, or 15 bytes instead of 17). The packed values are used internally for mask and comparison operations. find() and bin_find() use Perl string comparison (lt/gt) on these values, and comparing strings of different lengths gives wrong results. This can cause find() to incorrectly report an address as inside or outside a range. Example: my $cidr = Net::CIDR::Lite->new("::/8"); $cidr->find("1:2:3"); # invalid input, incorrectly returns true This is the same class of input validation issue as CVE-2021-47154 (IPv4 leading zeros) previously fixed in this module. See also CVE-2026-40199, a related issue in the same function affecting IPv4 mapped IPv6 addresses.	7.5	More Details
CVE-2025-45057	D-Link DI-8300 v16.07.26A1 was discovered to contain a buffer overflow via the ip parameter in the ip_position_asp function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-45058	D-Link DI-8300 v16.07.26A1 was discovered to contain a buffer overflow via the fx parameter in the jingx_asp function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-45059	D-Link DI-8300 v16.07.26A1 was discovered to contain a buffer overflow via the fn parameter in the tgfile_htm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-52222	D-Link DI-8003 v16.07.26A1, DI-8500 v16.07.26A1; DI-8003G v17.12.21A1, DI-8200G v17.12.20A1, DI-8200 v16.07.26A1, DI-8400 v16.07.26A1, DI-8004w v16.07.26A1, DI-8100 v16.07.26A1, and DI-8100G v17.12.20A1 were discovered to contain a buffer overflow via the rd_en, rd_auth, rd_acct, http_hadmin, http_hadminpwd, rd_key, and rd_ip parameters in the radius_asp function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2026-33710	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, REST API keys are generated using md5(time() + (user_id * 5) - rand(10000, 10000)). The rand(10000, 10000) call always returns exactly 10000 (min == max), making the formula effectively md5(timestamp + user_id*5 - 10000). An attacker who knows a username and approximate key creation time can brute-force the API key. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.5	More Details
CVE-2026-33756	Saleor is an e-commerce platform. From 2.0.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, Saleor supports query batching by submitting multiple GraphQL operations in a single HTTP request as a JSON array but wasn't enforcing any upper limit on the number of operations. This allowed an unauthenticated attacker to send a single HTTP request many operations (bypassing the per query complexity limit) to exhaust resources. This vulnerability is fixed in 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118.	7.5	More Details
CVE-2026-32178	Improper neutralization of special elements in .NET allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2025-50644	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper validation of user input in the qj.asp endpoint.	7.5	More Details
CVE-2025-50645	A vulnerability has been discovered in D-Link DI-8003 16.07.26A1, which can lead to a buffer overflow when the s parameter in the pppoe_list_opt.asp endpoint is manipulated. By sending a crafted request with an excessively large value for the s parameter, an attacker can trigger a buffer overflow condition.	7.5	More Details
CVE-2025-50646	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to insufficient input validation on the name parameter in the /qos_type_asp.asp endpoint.	7.5	More Details
CVE-2025-50647	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1, specifically in the handling of the wans parameter in the qos.asp endpoint.	7.5	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability		More

2026-39544	in themeStek LabtechCO labtechco allows PHP Local File Inclusion.This issue affects LabtechCO: from n/a through <= 8.3.	7.5	Details
CVE-2025-50673	A buffer overflow vulnerability exists in D-Link DI-8003 16.07.26A1 due to improper handling of the http_lanport parameter in the /webgl.asp endpoint.	7.5	More Details
CVE-2026-39859	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.25.3, liquidjs 10.25.0 documents root as constraining filenames passed to renderFile() and parseFile(), but top-level file loads do not enforce that boundary. A Liquid instance configured with an empty temporary directory as root can return the contents of arbitrary files. This vulnerability is fixed in 10.25.3.	7.5	More Details
CVE-2026-35525	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.25.3, for {% include %}, {% render %}, and {% layout %}, LiquidJS checks whether the candidate path is inside the configured partials or layouts roots before reading it. That check is path-based, not realpath-based. Because of that, a file like partials/link.liquid passes the directory containment check as long as its pathname is under the allowed root. If link.liquid is actually a symlink to a file outside the allowed root, the filesystem follows the symlink when the file is opened and LiquidJS renders the external target. So the restriction is applied to the path string that was requested, not to the file that is actually read. This matters in environments where an attacker can place templates or otherwise influence files under a trusted template root, including uploaded themes, extracted archives, mounted content, or repository-controlled template trees. This vulnerability is fixed in 10.25.3.	7.5	More Details
CVE-2026-35650	OpenClaw before 2026.3.22 contains an environment variable override handling vulnerability that allows attackers to bypass the shared host environment policy through inconsistent sanitization paths. Attackers can supply blocked or malformed override keys that slip through inconsistent validation to execute arbitrary code with unintended environment variables.	7.5	More Details
CVE-2026-34723	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, unauthenticated remote attackers were able to access the getting started endpoint to get access to sensitive internal entity data, even after the system setup was completed. This vulnerability is fixed in 7.0.1 and 6.5.4.	7.5	More Details
CVE-2025-69624	Nitro PDF Pro for Windows 14.41.1.4 contains a NULL pointer dereference vulnerability in the JavaScript implementation of app.alert(). When app.alert() is called with more than one argument and the first argument evaluates to null (for example, app.alert(app.activeDocs, true) when app.activeDocs is null), the engine routes the call through a fallback path intended for non-string arguments. In this path, js_ValueToString() is invoked on the null value and returns an invalid string pointer, which is then passed to JS_GetStringChars() without validation. Dereferencing this pointer leads to an access violation and application crash when opening a crafted PDF.	7.5	More Details
CVE-2026-35401	Saleor is an e-commerce platform. From 2.0.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, a malicious actor can include many GraphQL mutations or queries in a single API call using aliases or chaining multiple mutations, resulting in resource exhaustion. This vulnerability is fixed in 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118.	7.5	More Details
CVE-2026-23869	A denial of service vulnerability exists in React Server Components, affecting the following packages: react-server-dom-parcel, react-server-dom-turbopack and react-server-dom-webpack (versions 19.0.0 through 19.0.4, 19.1.0 through 19.1.5, and 19.2.0 through 19.2.4). The vulnerability is triggered by sending specially crafted HTTP requests to Server Function endpoints.The payload of the HTTP request causes excessive CPU usage for up to a minute ending in a thrown error that is catchable.	7.5	More Details
CVE-2026-23782	An issue was discovered in BMC Control-M/MFT 9.0.20 through 9.0.22. An API management endpoint allows unauthenticated users to obtain both an API identifier and its corresponding secret value. With these exposed secrets, an attacker could invoke privileged API operations, potentially leading to unauthorized access.	7.5	More Details
CVE-2026-6069	NASM’s disasm() function contains a stack based buffer overflow when formatting disassembly output, allowing an attacker triggered out-of-bounds write when `slen` exceeds the buffer capacity.	7.5	More Details
CVE-2026-39863	Kamailio is an open source implementation of a SIP Signaling Server. Prior to 6.1.1, 6.0.6, and 5.8.8, an out-of-bounds access in the core of Kamailio (formerly OpenSER and SER) allows remote attackers to cause a denial of service (process crash) via a specially crafted data packet sent over TCP. The issue impacts Kamailio instances having TCP or TLS listeners. This vulnerability is fixed in 5.1.1, 6.0.6, and 5.8.8.	7.5	More Details
CVE-2026-30999	A heap buffer overflow in the av_bprint_finalize() function of FFmpeg v8.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-34392	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 20.0.0 to before 27.0.3 and 28.0.1, a bug in the static file router can allow an attacker to traverse outside of the intended directory, allowing unintended files to be downloaded through the static, css, and js endpoints. This vulnerability is fixed in 27.0.3 and 28.0.1.	7.5	More Details
CVE-2026-6067	A heap buffer overflow vulnerability exists in the Netwide Assembler (NASM) due to a lack of bounds checking in the obj_directive() function. This vulnerability can be exploited by a user assembling a malicious .asm file, potentially leading to heap memory corruption, denial of service (crash), and arbitrary code execution.	7.5	More Details
	Denial of Service via Out of Memory vulnerability in Apache ActiveMQ Client, Apache ActiveMQ Broker, Apache ActiveMQ. ActiveMQ NIO SSL transports do not correctly handle TLSv1.3 handshake KeyUpdates triggered by clients.		

CVE-2026-39304	This makes it possible for a client to rapidly trigger updates which causes the broker to exhaust all its memory in the SSL engine leading to DoS. Note: TLS versions before TLSv1.3 (such as TLSv1.2) are broken but are not vulnerable to OOM. Previous TLS versions require a full handshake renegotiation which causes a connection to hang but not OOM. This is fixed as well. This issue affects Apache ActiveMQ Client: before 5.19.4, from 6.0.0 before 6.2.4; Apache ActiveMQ Broker: before 5.19.4, from 6.0.0 before 6.2.4; Apache ActiveMQ: before 5.19.4, from 6.0.0 before 6.2.4. Users are recommended to upgrade to version 6.2.4 or 5.19.5, which fixes the issue.	7.5	More Details
CVE-2025-5804	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Case Themes Case Theme User allows PHP Local File Inclusion.This issue affects Case Theme User: from n/a before 1.0.4.	7.5	More Details
CVE-2026-30998	An improper resource deallocation and closure vulnerability in the tools/zmqsend.c component of FFmpeg v8.0.1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted input file.	7.5	More Details
CVE-2026-30997	An out-of-bounds read in the read_global_param() function (libavcodec/av1dec.c) of FFmpeg v8.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2025-66769	A NULL pointer dereference in Nitro PDF Pro for Windows v14.41.1.4 allows attackers to cause a Denial of Service (DoS) via a crafted XFA packet.	7.5	More Details
CVE-2026-2332	In Eclipse Jetty, the HTTP/1.1 parser is vulnerable to request smuggling when chunk extensions are used, similar to the "funky chunks" techniques outlined here: * https://w4ke.info/2025/06/18/funky-chunks.html * https://w4ke.info/2025/10/29/funky-chunks-2.html Jetty terminates chunk extension parsing at \r\n inside quoted strings instead of treating this as an error. POST / HTTP/1.1 Host: localhost Transfer-Encoding: chunked 1;ext="val X 0 GET /smuggled HTTP/1.1 ... Note how the chunk extension does not close the double quotes, and it is able to inject a smuggled request.	7.4	More Details
CVE-2026-32156	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an unauthorized attacker to execute code locally.	7.4	More Details
CVE-2026-34727	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the OIDC callback handler issues a full JWT token without checking whether the matched user has TOTP two-factor authentication enabled. When a local user with TOTP enrolled is matched via the OIDC email fallback mechanism, the second factor is completely skipped. This vulnerability is fixed in 2.3.0.	7.4	More Details
CVE-2026-25207	Out-of-bounds write vulnerability in Samsung Open Source Escargot allows Overflow Buffers.This issue affects Escargot: 97e8115ab1110bc502b4b5e4a0c689a71520d335.	7.4	More Details
CVE-2026-33771	A Weak Password Requirements vulnerability in the password management function of Juniper Networks CTP OS might allow an unauthenticated, network-based attacker to exploit weak passwords of local accounts and potentially take full control of the device. The password management menu enables the administrator to set password complexity requirements, but these settings are not saved. The issue can be verified with the menu option "Show password requirements". Failure to enforce the intended requirements can lead to weak passwords being used, which significantly increases the likelihood that an attacker can guess these and subsequently attain unauthorized access. This issue affects CTP OS versions 9.2R1 and 9.2R2.	7.4	More Details
CVE-2026-25205	Heap-based buffer overflow vulnerability in Samsung Open Source Escargot allows out-of-bounds write.This issue affects Escargot:commit hash 97e8115ab1110bc502b4b5e4a0c689a71520d335 .	7.4	More Details
CVE-2026-40153	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, the execute_command function in shell_tools.py calls os.path.expandvars() on every command argument at line 64, manually re-implementing shell-level environment variable expansion despite using shell=False (line 88) for security. This allows exfiltration of secrets stored in environment variables (database credentials, API keys, cloud access keys). The approval system displays the unexpanded $VAR references to human reviewers, creating a deceptive approval where the displayed command differs from what actually executes. This vulnerability is fixed in 1.5.128.	7.4	More Details
CVE-2026-5795	In Eclipse Jetty, the class JASPIAuthenticator initiates the authentication checks, which set two ThreadLocal variable. Upon returning from the initial checks, there are conditions that cause an early return from the JASPIAuthenticator code without clearing those ThreadLocals. A subsequent request using the same thread inherits the ThreadLocal values, leading to a broken access control and privilege escalation.	7.4	More Details
CVE-2026-33797	An Improper Input Validation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker, sending a specific genuine BGP packet in an already established BGP session to reset only that session causing a Denial of Service (DoS). An attacker repeatedly sending the packet will sustain the Denial of Service (DoS).This issue affects Junos OS: * 25.2 versions before 25.2R2 This issue doesn't not affected Junos OS versions before 25.2R1. This issue affects Junos OS Evolved: * 25.2-EVO versions before 25.2R2-EVO This issue doesn't not affected Junos OS Evolved versions before 25.2R1-EVO. eBGP and iBGP are affected. IPv4 and IPv6 are affected.	7.4	More Details
CVE-2026-	OpenClaw before 2026.3.25 contains a server-side request forgery vulnerability in multiple channel extensions that fail to properly guard configured base URLs against SSRF attacks. Attackers can exploit unprotected fetch() calls	7.4	More

35629	against configured endpoints to rebind requests to blocked internal destinations and access restricted resources.		Details
CVE-2026-33021	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. Versions 1.8.7 and prior contain a use-after-free vulnerability in sixel_encoder_encode_bytes() because sixel_frame_init() stores the caller-owned pixel buffer pointer directly in frame->pixels without making a defensive copy. When a resize operation is triggered, sixel_frame_convert_to_rgb888() unconditionally frees this caller-owned buffer and replaces it with a new internal allocation, leaving the caller with a dangling pointer. Any subsequent access to the original buffer by the caller constitutes a use-after-free, confirmed by AddressSanitizer. An attacker who controls incoming frames can trigger this bug repeatedly and predictably, resulting in a reliable crash with potential for code execution. This issue has been fixed in version 1.8.7-r1.	7.3	More Details
CVE-2026-5970	A vulnerability was detected in FoundationAgents MetaGPT up to 0.8.1. This affects the function check_solution of the component HumanEvalBenchmark/MBPPBenchmark. Performing a manipulation results in code injection. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	7.3	More Details
CVE-2026-6142	A vulnerability was identified in tushar-2223 Hotel Management System up to bb1f3b3666124b888f1e4bcf51b6fba9fbb01d15. Affected by this vulnerability is an unknown functionality of the file /admin/roomdelete.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. 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.	7.3	More Details
CVE-2026-5814	A security vulnerability has been detected in PHPGurukul Online Course Registration 3.1. This issue affects some unknown processing of the file /admin/check_availability.php. The manipulation of the argument regno leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-5813	A weakness has been identified in PHPGurukul Online Course Registration 3.1. This vulnerability affects unknown code of the file /check_availability.php. Executing a manipulation of the argument cid can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-5837	A vulnerability was found in PHPGurukul News Portal Project 4.1. This affects an unknown part of the file /news-details.php. The manipulation of the argument Comment results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-6038	A vulnerability was identified in code-projects Vehicle Showroom Management System 1.0. This impacts an unknown function of the file /util/RegisterCustomerFunction.php. Such manipulation of the argument BRANCH_ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-6151	A vulnerability was found in code-projects Vehicle Showroom Management System 1.0. This vulnerability affects unknown code of the file /util/PaymentStatusFunction.php. The manipulation of the argument CUSTOMER_ID results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-5971	A flaw has been found in FoundationAgents MetaGPT up to 0.8.1. This vulnerability affects the function ActionNode.xml_fill of the file metagpt/actions/action_node.py of the component XML Handler. Executing a manipulation can lead to improper neutralization of directives in dynamically evaluated code. The attack may be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	7.3	More Details
CVE-2026-5824	A security vulnerability has been detected in code-projects Simple Laundry System 1.0. This affects an unknown part of the file /userchecklogin.php. Such manipulation of the argument userid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-6149	A flaw has been found in code-projects Vehicle Showroom Management System 1.0. Affected by this issue is some unknown functionality of the file /util/BookVehicleFunction.php. Executing a manipulation of the argument BRANCH_ID can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	7.3	More Details
CVE-2026-6031	A vulnerability has been found in code-projects Simple IT Discussion Forum 1.0. This affects an unknown function of the file /add-category-function.php. Such manipulation of the argument Category leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-6148	A vulnerability was detected in code-projects Vehicle Showroom Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /util/MonthTotalReportUpdateFunction.php. Performing a manipulation of the argument BRANCH_ID results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-6126	A weakness has been identified in zhayujie chatgpt-on-wechat CowAgent 2.0.4. The affected element is an unknown function of the component Administrative HTTP Endpoint. This manipulation causes missing authentication. It is possible to initiate the attack 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-2026-6158	A flaw has been found in Totolink N300RH 6.1c.1353_B20190305. Affected is the function setUpgradeUboot of the file upgrade.so. This manipulation of the argument FileName causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	7.3	More Details
CVE-	A vulnerability was determined in Tenda i6 1.0.0.7(2204). Affected by this issue is the function		

2026-6024	R7WebsSecurityHandlerfunction of the component HTTP Handler. This manipulation causes path traversal. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-6105	A security vulnerability has been detected in perfree go-fastdfs-web up to 1.3.7. This affects an unknown part of the file src/main/java/com/perfree/controller/InstallController.java of the component doInstall Interface. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-5827	A vulnerability has been found in code-projects Simple IT Discussion Forum 1.0. Impacted is an unknown function of the file /question-function.php. The manipulation of the argument content leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-6152	A vulnerability was determined in code-projects Vehicle Showroom Management System 1.0. This issue affects some unknown processing of the file /util/StaffAddingFunction.php. This manipulation of the argument STAFF_ID causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-6110	A vulnerability was identified in FoundationAgents MetaGPT up to 0.8.1. This affects the function generate_thoughts of the file metagpt/strategy/tot.py of the component Tree-of-Thought Solver. The manipulation leads to code injection. It is possible to initiate the attack 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.	7.3	More Details
CVE-2026-5828	A vulnerability was found in code-projects Simple IT Discussion Forum 1.0. The affected element is an unknown function of the file /functions/addcomment.php. The manipulation of the argument postid results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-34856	UAF vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	7.3	More Details
CVE-2026-5829	A vulnerability was determined in code-projects Simple IT Discussion Forum 1.0. The impacted element is an unknown function of the file /pages/content.php. This manipulation of the argument post_id causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-5961	A security vulnerability has been detected in code-projects Simple IT Discussion Forum 1.0. This vulnerability affects unknown code of the file /topic-details.php. The manipulation of the argument post_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-5962	A vulnerability was detected in Tenda CH22 1.0.0.6(468). This issue affects the function R7WebsSecurityHandlerfunction of the component httpd. The manipulation results in path traversal. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-6161	A vulnerability was determined in code-projects Simple ChatBox up to 1.0. This affects an unknown part of the file /chatbox/insert.php of the component Endpoint. Executing a manipulation of the argument msg can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-5832	A weakness has been identified in atototo api-lab-mcp up to 0.2.1. This affects the function analyze_api_spec/generate_test_scenarios/test_http_endpoint of the file src/mcp/http-server.ts of the component HTTP Interface. This manipulation of the argument source/url causes server-side request forgery. 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.	7.3	More Details
CVE-2026-6153	A vulnerability was identified in code-projects Vehicle Showroom Management System 1.0. Impacted is an unknown function of the file /util/StaffDetailsFunction.php. Such manipulation of the argument STAFF_ID leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-5802	A vulnerability was identified in idachev mcp-javadc up to 1.2.4. Impacted is an unknown function of the component HTTP Interface. Such manipulation of the argument jarFilePath leads to os command injection. It is possible to launch the attack 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.	7.3	More Details
CVE-2026-6004	A vulnerability was detected in code-projects Simple IT Discussion Forum 1.0. Impacted is an unknown function of the file /delete-category.php. Performing a manipulation of the argument cat_id 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-2026-6193	A security flaw has been discovered in PHPGurukul Daily Expense Tracking System 1.1. Affected is an unknown function of the file /register.php. The manipulation of the argument email results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-6163	A vulnerability was identified in code-projects Lost and Found Thing Management 1.0. Affected by this issue is some unknown functionality of the file /catageory.php. Such manipulation of the argument cat 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-2026-6167	A vulnerability was detected in code-projects Faculty Management System 1.0. Impacted is an unknown function of the file /subject-print.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
	A security vulnerability has been detected in code-projects Vehicle Showroom Management System 1.0. This issue		

CVE-2026-6166	affects some unknown processing of the file /util/UpdateVehicleFunction.php. The manipulation of the argument VEHICLE_ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-32149	Improper input validation in Windows Hyper-V allows an authorized attacker to execute code locally.	7.3	More Details
CVE-2026-6165	A weakness has been identified in code-projects Vehicle Showroom Management System 1.0. This vulnerability affects unknown code of the file /util/Login_check.php. Executing a manipulation of the argument ID 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.	7.3	More Details
CVE-2026-6130	A flaw has been found in chatboxai chatbox up to 1.20.0. This impacts the function StdioClientTransport of the file src/main/mcp/ipc-stdio-transport.ts of the component Model Context Protocol Server Management System. Executing a manipulation of the argument args/env can lead to os command injection. The attack can be launched 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.	7.3	More Details
CVE-2026-24032	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP3 with UMC). The affected application contains an authentication weakness due to insufficient validation of user identity in the UMC component. This could allow an unauthenticated remote attacker to bypass authentication and gain unauthorized access to the application. (ZDI-CAN-27564)	7.3	More Details
CVE-2026-6182	A vulnerability was identified in code-projects Simple Content Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /web/admin/login.php. Such manipulation of the argument User leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-35637	OpenClaw before 2026.3.22 performs cite expansion before completing channel and DM authorization checks, allowing cite work and content handling prior to final auth decisions. Attackers can exploit this timing vulnerability to access or manipulate content before proper authorization validation occurs.	7.3	More Details
CVE-2026-6129	A vulnerability was detected in zhayujie chatgpt-on-wechat CowAgent up to 2.0.4. This affects an unknown function of the component Agent Mode Service. Performing a manipulation results in missing authentication. The attack can be initiated 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.	7.3	More Details
CVE-2026-6183	A security flaw has been discovered in code-projects Simple Content Management System 1.0. Affected by this issue is some unknown functionality of the file /web/index.php. Performing a manipulation of the argument ID results in sql injection. 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-2026-5985	A security flaw has been discovered in code-projects Simple IT Discussion Forum 1.0. The affected element is an unknown function of the file /crud.php. The manipulation of the argument user_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.	7.3	More Details
CVE-2026-6036	A vulnerability was found in code-projects Vehicle Showroom Management System 1.0. The impacted element is an unknown function of the file /util/VehicleDetailsFunction.php. The manipulation of the argument VEHICLE_ID results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-6224	A security flaw has been discovered in nocobase plugin-workflow-javascript up to 2.0.23. This issue affects the function createSafeConsole of the file packages/plugins/@nocobase/plugin-workflow-javascript/src/server/Vm.js. Performing a manipulation results in sandbox issue. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-21916	A UNIX Symbolic Link (Symlink) Following vulnerability in the CLI of Juniper Networks Junos OS allows a local, authenticated attacker with low privileges to escalate their privileges to root which will lead to a complete compromise of the system. When after a user has performed a specific 'file link ...' CLI operation, another user commits (unrelated configuration changes), the first user can login as root. This issue affects Junos OS: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R2. This issue does not affect versions 25.4R1 or later.	7.3	More Details
CVE-2026-6037	A vulnerability was determined in code-projects Vehicle Showroom Management System 1.0. This affects an unknown function of the file /util/AddVehicleFunction.php. This manipulation of the argument BRANCH_ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-6187	A vulnerability was detected in SourceCodester Pharmacy Sales and Inventory System 1.0. This issue affects some unknown processing of the file /ajax.php?action=chk_prod_availability. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-6164	A security flaw has been discovered in code-projects Lost and Found Thing Management 1.0. This affects an unknown part of the file /addcat.php. Performing a manipulation of the argument cata 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-	A weakness has been identified in code-projects Easy Blog Site up to 1.0. The impacted element is an unknown function of the file /users/contact_us.php. Executing a manipulation of the argument Name can lead to sql injection.		More

2026-5805	The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.3	Details
CVE-2026-5842	A security vulnerability has been detected in decolua 9router up to 0.3.47. The impacted element is an unknown function of the file /api of the component Administrative API Endpoint. The manipulation leads to authorization bypass. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.3.75 is sufficient to resolve this issue. It is suggested to upgrade the affected component.	7.3	More Details
CVE-2026-5972	A vulnerability has been found in FoundationAgents MetaGPT up to 0.8.1. This issue affects the function Terminal.run_command in the library metagpt/tools/libs/terminal.py. The manipulation leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The identifier of the patch is d04ffc8dc67903e8b327f78ec121df5e190ffc7b. Applying a patch is the recommended action to fix this issue.	7.3	More Details
CVE-2026-5973	A vulnerability was found in FoundationAgents MetaGPT up to 0.8.1. Impacted is the function get_mime_type of the file metagpt/utils/common.py. The manipulation results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used. The project was informed of the problem early through a pull request but has not reacted yet.	7.3	More Details
CVE-2026-6189	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. The affected element is an unknown function of the file /ajax.php?action=login. 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.	7.3	More Details
CVE-2026-36948	Sourcecodester Online Thesis Archiving System v1.0 is vulnerale to SQL injection in the file /otas/view_archive.php.	7.3	More Details
CVE-2026-40027	ALEAPP (Android Logs Events And Protobuf Parser) through 3.4.0 contains a path traversal vulnerability in the NQ_Vault.py artifact parser that uses attacker-controlled file_name_from values from a database directly as the output filename, allowing arbitrary file writes outside the report output directory. An attacker can embed a path traversal payload such as ../../../outside_written.bin in the database to write files to arbitrary locations, potentially achieving code execution by overwriting executable files or configuration.	7.3	More Details
CVE-2026-5974	A vulnerability was determined in FoundationAgents MetaGPT up to 0.8.1. The affected element is the function Bash.run in the library metagpt/tools/libs/terminal.py. This manipulation causes os command injection. The attack is possible to be carried out remotely. The project was informed of the problem early through a pull request but has not reacted yet.	7.3	More Details
CVE-2026-5849	A vulnerability was determined in Tenda i12 1.0.0.11(3862). The impacted element is an unknown function of the component HTTP Handler. Executing a manipulation can lead to path traversal. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-35455	immich is a high performance self-hosted photo and video management solution. Prior to 2.7.0, sStored Cross-Site Scripting (XSS) in the 360° panorama viewer allows any authenticated user to execute arbitrary JavaScript in the browser of any other user who views the malicious panorama with the OCR overlay enabled. The attacker uploads an equirectangular image containing crafted text; OCR extracts it, and the panorama viewer renders it via innerHTML without sanitization. This enables session hijacking (via persistent API key creation), private photo exfiltration, and access to GPS location history and face biometric data. This vulnerability is fixed in 2.7.0.	7.3	More Details
CVE-2026-6188	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Impacted is an unknown function of the file /ajax.php?action=delete_sales. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-5841	A weakness has been identified in Tenda i3 1.0.0.6(2204). The affected element is the function R7WebsSecurityHandler of the component HTTP Handler. Executing a manipulation can lead to path traversal. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-4113	An observable response discrepancy vulnerability in the SonicWall SMA1000 series appliances allows a remote attacker to enumerate SSL VPN user credentials.	7.2	More Details
CVE-2026-4116	Improper handling of Unicode encoding in SonicWall SMA1000 series appliances allows a remote authenticated SSLVPN user to bypass Workplace/Connect Tunnel TOTP authentication.	7.2	More Details
CVE-2025-61848	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.8, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.8, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.8, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.8, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow a privileged authenticated attacker to execute unauthorized code or commands via JSON RPC API	7.2	More Details
	BoidCMS is an open-source, PHP-based flat-file CMS for building simple websites and blogs, using JSON as its database. Versions prior to 2.1.3 are vulnerable to a critical Local File Inclusion (LFI) attack via the tpl parameter, which can lead to Remote Code Execution (RCE).The application fails to sanitize the tpl (template) parameter during		

CVE-2026-39387	page creation and updates. This parameter is passed directly to a require_once() statement without path validation. An authenticated administrator can exploit this by injecting path traversal sequences (../) into the tpl value to escape the intended theme directory and include arbitrary files — specifically, files from the server's media/ directory. When combined with the file upload functionality, this becomes a full RCE chain: an attacker can first upload a file with embedded PHP code (e.g., disguised as image data), then use the path traversal vulnerability to include that file via require_once(), executing the embedded code with web server privileges. This issue has been fixed in version 2.1.3.	7.2	More Details
CVE-2026-5217	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.2.2. This is due to insufficient input sanitization and output escaping on the user-supplied 's' parameter (srcset descriptor) in the unauthenticated /wp-json/optimole/v1/optimizations REST endpoint. The endpoint validates requests using an HMAC signature and timestamp, but these values are exposed directly in the frontend HTML making them accessible to any visitor. The plugin uses sanitize_text_field() on the descriptor value of rest.php, which strips HTML tags but does not escape double quotes. The poisoned descriptor is then stored via transients (backed by the WordPress options table) and later retrieved and injected verbatim into the srcset attribute of tag_replacer.php without proper escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts into pages that will execute whenever a user accesses the injected page.	7.2	More Details
CVE-2026-40038	Pachno 1.0.6 contains a stored cross-site scripting vulnerability that allows attackers to execute arbitrary HTML and script code by injecting malicious payloads into POST parameters. Attackers can inject scripts through the value, comment_body, article_content, description, and message parameters across multiple controllers, which are stored in the database and executed in users' browser sessions due to improper sanitization via Request::getRawParameter() or Request::getParameter() calls.	7.2	More Details
CVE-2026-29002	CouchCMS contains a privilege escalation vulnerability that allows authenticated Admin-level users to create SuperAdmin accounts by tampering with the f_k_levels_list parameter in user creation requests. Attackers can modify the parameter value from 4 to 10 in the HTTP request body to bypass authorization validation and gain full application control, circumventing restrictions on SuperAdmin account creation and privilege assignment.	7.2	More Details
CVE-2026-33715	Chamilo LMS is an open-source learning management system. In version 2.0-RC.2, the file public/main/inc/ajax/install.ajax.php is accessible without authentication on fully installed instances because, unlike other AJAX endpoints, it does not include the global.inc.php file that performs authentication and installation-completed checks. Its test_mailer action accepts an arbitrary Symfony Mailer DSN string from POST data and uses it to connect to an attacker-specified SMTP server, enabling Server-Side Request Forgery (SSRF) into internal networks via the SMTP protocol. An unauthenticated attacker can also abuse this to weaponize the Chamilo server as an open email relay for phishing and spam campaigns, with emails appearing to originate from the server's IP address. Additionally, error responses from failed SMTP connections may disclose information about internal network topology and running services. This issue has been fixed in version 2.0.0-RC.3.	7.2	More Details
CVE-2026-4388	The Form Maker by 10Web plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Matrix field (Text Box input type) in form submissions in all versions up to, and including, 1.15.40. This is due to insufficient input sanitization (`sanitize_text_field` strips tags but not quotes) and missing output escaping when rendering submission data in the admin Submissions view. This makes it possible for unauthenticated attackers to inject arbitrary JavaScript through a form submission that executes in the browser of an administrator who views the submission details.	7.2	More Details
CVE-2026-6227	The BackWPup plugin for WordPress is vulnerable to Local File Inclusion via the `block_name` parameter of the `/wp-json/backwpup/v1/getblock` REST endpoint in all versions up to, and including, 5.6.6 due to a non-recursive `str_replace()` sanitization of path traversal sequences. This makes it possible for authenticated attackers, with Administrator-level access and above, to include arbitrary PHP files on the server via crafted traversal sequences (e.g., `....//`), which can be leveraged to read sensitive files such as `wp-config.php` or achieve remote code execution in certain configurations. Administrators have the ability to grant individual users permission to handle backups, which may then allow lower-level users to exploit this vulnerability.	7.2	More Details
CVE-2026-3017	The Smart Post Show – Post Grid, Post Carousel & Slider, and List Category Posts plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.0.12 via deserialization of untrusted input in the import_shortcodes() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	7.2	More Details
CVE-2026-40114	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the /api/v1/runs endpoint accepts an arbitrary webhook_url in the request body with no URL validation. When a submitted job completes (success or failure), the server makes an HTTP POST request to this URL using httpx.AsyncClient. An unauthenticated attacker can use this to make the server send POST requests to arbitrary internal or external destinations, enabling SSRF against cloud metadata services, internal APIs, and other network-adjacent services. This vulnerability is fixed in 4.5.128.	7.2	More Details
CVE-2026-40242	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.17.3, the /api/templates/fetch endpoint accepts a caller-supplied url parameter and performs a server-side HTTP GET request to that URL without authentication and without URL scheme or host validation. The server's response is returned directly to the caller. type. This constitutes an unauthenticated SSRF vulnerability affecting any publicly reachable Arcane instance. This vulnerability is fixed in 1.17.3.	7.2	More Details
CVE-2026-40688	A out-of-bounds write vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	7.2	More Details

CVE-2026-35476	InvenTree is an Open Source Inventory Management System. Prior to 1.2.7 and 1.3.0, a non-staff authenticated user can elevate their account to a staff level via a POST request against their user account endpoint. The write permissions on the API endpoint are improperly configured, allowing any user to change their staff status. This vulnerability is fixed in 1.2.7 and 1.3.0.	7.2	More Details
CVE-2026-5844	A vulnerability was found in D-Link DIR-882 1.01B02. Impacted is the function sprintf of the file prog.cgi of the component HNAP1 SetNetworkSettings Handler. The manipulation of the argument IPAddress results in os command injection. The attack may be performed from remote. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2024-1490	An authenticated remote attacker with high privileges can exploit the OpenVPN configuration via the web-based management interface of a WAGO PLC. If user-defined scripts are permitted, OpenVPN may allow the execution of arbitrary shell commands enabling the attacker to run arbitrary commands on the device.	7.2	More Details
CVE-2026-4808	The Gerador de Certificados – DevApps plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the moveUploadedFile() function in all versions up to, and including, 1.3.6. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2026-1343	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 allows an attacker to contact internal authentication endpoints which are protected by the Reverse Proxy.	7.2	More Details
CVE-2026-32188	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	7.1	More Details
CVE-2026-32894	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the gradebook result view page allows any authenticated teacher to delete any student's grade result across the entire platform by manipulating the delete_mark or resultdelete GET parameters. No ownership or course-scope verification is performed. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.1	More Details
CVE-2026-32930	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the gradebook evaluation edit page allows any authenticated teacher to view and modify the settings (name, max score, weight) of evaluations belonging to any other course by manipulating the editeval GET parameter. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.1	More Details
CVE-2026-40162	Bugsink is a self-hosted error tracking tool. In 2.1.0, an authenticated file write vulnerability was identified in Bugsink 2.1.0 in the artifact bundle assembly flow. A user with a valid authentication token could cause the application to write attacker-controlled content to a filesystem location writable by the Bugsink process. This vulnerability is fixed in 2.1.1.	7.1	More Details
CVE-2026-33702	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, Chamilo LMS contains an Insecure Direct Object Reference (IDOR) vulnerability in the Learning Path progress saving endpoint. The file lp_ajax_save_item.php accepts a uid (user ID) parameter directly from $_REQUEST and uses it to load and modify another user's Learning Path progress — including score, status, completion, and time — without verifying that the requesting user matches the target user ID. Any authenticated user enrolled in a course can overwrite another user's Learning Path progress by simply changing the uid parameter in the request. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	7.1	More Details
CVE-2026-33706	Chamilo LMS is a learning management system. Prior to 1.11.38, any authenticated user with a REST API key can modify their own status field via the update_user_from_username endpoint. A student (status=5) can change their status to Teacher/CourseManager (status=1), gaining course creation and management privileges. This vulnerability is fixed in 1.11.38.	7.1	More Details
CVE-2026-33019	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. Versions 1.8.7 and prior contain an integer overflow leading to an out-of-bounds heap read in the --crop option handling of img2sixel, where positive coordinates up to INT_MAX are accepted without overflow-safe bounds checking. In sixel_encoder_do_clip(), the expression clip_w + clip_x overflows to a large negative value when clip_x is INT_MAX, causing the bounds guard to be skipped entirely, and the unclamped coordinate is passed through sixel_frame_clip() to clip(), which computes a source pointer far beyond the image buffer and passes it to memmove(). An attacker supplying a specially crafted crop argument with any valid image can trigger an out-of-bounds read in the heap, resulting in a reliable crash and potential information disclosure. This issue has been fixed in version 1.8.7-r1.	7.1	More Details
CVE-2026-33020	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. Versions 1.8.7 and prior contain an integer overflow which leads to a heap buffer overflow via sixel_frame_convert_to_rgb888() in frame.c, where allocation size and pointer offset computations for palettised images (PAL1, PAL2, PAL4) are performed using int arithmetic before casting to size_t. For images whose pixel count exceeds INT_MAX / 4, the overflow produces an undersized heap allocation for the conversion buffer and a negative pointer offset for the normalization sub-buffer, after which sixel_helper_normalize_pixelformat() writes the full image data starting from the invalid pointer, causing massive heap corruption confirmed by ASAN. An attacker providing a specially crafted large palettised PNG can corrupt the heap of the victim process, resulting in a reliable crash and potential arbitrary code execution. This issue has been fixed in version 1.8.7-r1.	7.1	More Details
CVE-	Tmds.DBus provides .NET libraries for working with D-Bus from .NET. Tmds.DBus and Tmds.DBus.Protocol are vulnerable to malicious D-Bus peers. A peer on the same bus can spoof signals by impersonating the owner of a well-		

2026-39959	known name, exhaust system resources or cause file descriptor spillover by sending messages with an excessive number of Unix file descriptors, and crash the application by sending malformed message bodies that cause unhandled exceptions on the SynchronizationContext. This vulnerability is fixed in Tmds.DBus 0.92.0 and Tmds.DBus.Protocol 0.92.0 and 0.21.3.	7.1	More Details
CVE-2019-25713	MyT-PM 1.5.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the Charge[group_total] parameter. Attackers can submit crafted POST requests to the /charge/admin endpoint with error-based, time-based blind, or stacked query payloads to extract sensitive database information or manipulate data.	7.1	More Details
CVE-2026-33704	Chamilo LMS is a learning management system. Prior to 1.11.38, any authenticated user (including students) can write arbitrary content to files on the server via the BigUpload endpoint. The key parameter controls the filename and the raw POST body becomes the file content. While .php extensions are filtered to .phps, the .pht extension passes through unmodified. On Apache configurations where .pht is handled as PHP, this leads to Remote Code Execution. This vulnerability is fixed in 1.11.38.	7.1	More Details
CVE-2026-39976	Laravel Passport provides OAuth2 server support to Laravel. From 13.0.0 to before 13.7.1, there is an Authentication Bypass for client_credentials tokens. the league/oauth2-server library sets the JWT sub claim to the client identifier (since there's no user). The token guard then passes this value to retrieveById() without validating it's actually a user identifier, potentially resolving an unrelated real user. Any machine-to-machine token can inadvertently authenticate as an actual user. This vulnerability is fixed in 13.7.1.	7.1	More Details
CVE-2026-40436	The ZTE ZXEDM iEMS product has a password reset vulnerability for any user.Because the management of the cloud EMS portal does not properly control access to the user list acquisition function, attackers can read all user list information through the user list interface. Attackers can reset the passwords of obtained user information, causing risks such as unauthorized operations.	7.1	More Details
CVE-2019-25703	ImpressCMS 1.3.11 contains a time-based blind SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'bid' parameter. Attackers can send POST requests to the admin.php endpoint with malicious 'bid' values containing SQL commands to extract sensitive database information.	7.1	More Details
CVE-2019-25699	Newsbull Haber Script 1.0.0 contains multiple SQL injection vulnerabilities in the search parameter that allow authenticated attackers to extract database information through time-based, blind, and boolean-based injection techniques. Attackers can inject malicious SQL code through the search parameter in endpoints like /admin/comment/records, /admin/category/records, /admin/news/records, and /admin/menu/childs to manipulate database queries and retrieve sensitive data.	7.1	More Details
CVE-2019-25693	ResourceSpace 8.6 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the keywords parameter in collection_edit.php. Attackers can submit POST requests with crafted SQL payloads in the keywords field to extract sensitive database information including schema names, user credentials, and other confidential data.	7.1	More Details
CVE-2026-40185	TREK is a collaborative travel planner. Prior to 2.7.2, TREK was missing authorization checks on the Immich trip photo management routes. This vulnerability is fixed in 2.7.2.	7.1	More Details
CVE-2018-25257	Adianti Framework 5.5.0 and 5.6.0 contains an SQL injection vulnerability that allows authenticated users to manipulate database queries by injecting SQL code through the name field in SystemProfileForm. Attackers can submit crafted SQL statements in the profile edit endpoint to modify user credentials and gain administrative access.	7.1	More Details
CVE-2026-32590	A flaw was found in Red Hat Quay's handling of resumable container image layer uploads. The upload process stores intermediate data in the database using a format that, if tampered with, could allow an attacker to execute arbitrary code on the Quay server.	7.1	More Details
CVE-2026-34602	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, the /api/course_rel_users endpoint is vulnerable to Insecure Direct Object Reference (IDOR), allowing an authenticated attacker to modify the user parameter in the request body to enroll any arbitrary user into any course without proper authorization checks. The backend trusts the user-supplied input for the user field and performs no server-side verification that the requester owns the referenced user ID or has permission to act on behalf of other users. This enables unauthorized manipulation of user-course relationships, potentially granting unintended access to course materials, bypassing enrollment controls, and compromising platform integrity. This issue has been fixed in version 2.0.0-RC.3.	7.1	More Details
CVE-2026-32589	A flaw was found in Red Hat Quay's container image upload process. An authenticated user with push access to any repository on the registry can interfere with image uploads in progress by other users, including those in repositories they do not have access to. This could allow the attacker to read, modify, or cancel another user's in-progress image upload.	7.1	More Details
CVE-2026-5809	The wpForo Forum plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to and including 3.0.2. This is due to a two-step logic flaw: the topic_add() and topic_edit() action handlers accept arbitrary user-supplied data[*] arrays from $_REQUEST and store them as postmeta without restricting which fields may contain array values. Because 'body' is included in the allowed topic fields list, an attacker can supply data[body][fileurl] with an arbitrary file path (e.g., wp-config.php or an absolute server path). This poisoned fileurl is persisted to the plugin's custom postmeta database table. Subsequently, when the attacker submits wpftcf_delete[]=body on a topic_edit request, the add_file() method retrieves the stored postmeta record, extracts the attacker-controlled fileurl, passes it through wpforo_fix_upload_dir() which only rewrites legitimate wpforo upload paths and returns all other paths unchanged,	7.1	More Details

	and then calls wp_delete_file() on the unvalidated path. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files writable by the PHP process on the server, including critical files such as wp-config.		
CVE-2019-25707	eBrigade ERP 4.5 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to pdf.php with crafted SQL payloads in the 'id' parameter to extract sensitive database information including table names and schema details.	7.1	More Details
CVE-2026-27144	The compiler is meant to unwrap pointers which are the operands of a memory move; a no-op interface conversion prevented the compiler from making the correct determination about non-overlapping moves, potentially leading to memory corruption at runtime.	7.1	More Details
CVE-2026-5441	An out-of-bounds read vulnerability exists in the `DecodePsmctRle1` function of `DicomImageDecoder.cpp`. The `PMSCT_RLE1` decompression routine, which decodes the proprietary Philips Compression format, does not properly validate escape markers placed near the end of the compressed data stream. A crafted sequence at the end of the buffer can cause the decoder to read beyond the allocated memory region and leak heap data into the rendered image output.	7.1	More Details
CVE-2026-35632	OpenClaw through 2026.2.22 contains a symlink traversal vulnerability in agents.create and agents.update handlers that use fs.appendFile on IDENTITY.md without symlink containment checks. Attackers with workspace access can plant symlinks to append attacker-controlled content to arbitrary files, enabling remote code execution via crontab injection or unauthorized access via SSH key manipulation.	7.1	More Details
CVE-2026-38528	Krayin CRM v2.2.x was discovered to contain a SQL injection vulnerability via the rotten_lead parameter at /Lead/LeadDataGrid.php.	7.1	More Details
CVE-2026-39671	Cross-Site Request Forgery (CSRF) vulnerability in Dotstore Extra Fees Plugin for WooCommerce woo-conditional-product-fees-for-checkout allows Cross Site Request Forgery.This issue affects Extra Fees Plugin for WooCommerce: from n/a through <= 4.3.3.	7.1	More Details
CVE-2026-34256	Due to a missing authorization check in SAP ERP and SAP S/4HANA (Private Cloud and On-Premise), an authenticated attacker could execute a particular ABAP report to overwrite any existing eight?character executable ABAP report without authorization. If the overwritten report is subsequently executed, the intended functionality could become unavailable. Successful exploitation impacts availability, with a limited impact on integrity confined to the affected report, while confidentiality remains unaffected.	7.1	More Details
CVE-2026-4369	A maliciously crafted HTML payload in an assembly variant name, when displayed during the delete confirmation dialog and clicked by a user, can trigger a Stored Cross-site Scripting (XSS) vulnerability in the Autodesk Fusion desktop application. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	7.1	More Details
CVE-2026-5444	A heap buffer overflow vulnerability exists in the PAM image parsing logic. When Orthanc processes a crafted PAM image embedded in a DICOM file, image dimensions are multiplied using 32-bit unsigned arithmetic. Specially chosen values can cause an integer overflow during buffer size calculation, resulting in the allocation of a small buffer followed by a much larger write operation during pixel processing.	7.1	More Details
CVE-2026-4345	A maliciously crafted HTML payload, stored in a design name and exported to CSV, can trigger a Stored Cross-site Scripting (XSS) vulnerability in the Autodesk Fusion desktop application. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	7.1	More Details
CVE-2026-4344	A maliciously crafted HTML payload in a component name, when displayed during the delete confirmation dialog and clicked by a user, can trigger a Stored Cross-site Scripting (XSS) vulnerability in the Autodesk Fusion desktop application. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	7.1	More Details
CVE-2026-33892	A vulnerability has been identified in Industrial Edge Management Pro V1 (All versions >= V1.7.6 < V1.15.17), Industrial Edge Management Pro V2 (All versions >= V2.0.0 < V2.1.1), Industrial Edge Management Virtual (All versions >= V2.2.0 < V2.8.0). Affected management systems do not properly enforce user authentication on remote connections to devices. This could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user. Successful exploitation requires that the attacker has identified the header and port used for remote connections to devices and that the remote connection feature is enabled for the device. Exploitation allows the attacker to tunnel to the device. Security features on this device itself (e.g. app specific authentication) are not affected.	7.1	More Details
CVE-2026-26151	Insufficient ui warning of dangerous operations in Windows Remote Desktop allows an unauthorized attacker to perform spoofing over a network.	7.1	More Details
CVE-2026-4162	The Gravity SMTP plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.1.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to uninstall and deactivate the plugin and delete plugin options. NOTE: This vulnerability is also exploitable via a Cross-Site Request Forgery vector.	7.1	More Details
CVE-2026-	Server-Side Request Forgery via SW-URL Header vulnerability in Apache SkyWalking MCP. This issue affects Apache	7.1	More

34476	SkyWalking MCP: 0.1.0. Users are recommended to upgrade to version 0.2.0, which fixes this issue.		Details
CVE-2025-58920	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zootemplate Cerato allows Reflected XSS.This issue affects Cerato: from n/a through 2.2.18.	7.1	More Details
CVE-2026-40024	The Sleuth Kit through 4.14.0 contains a path traversal vulnerability in tsk_recover that allows an attacker to write files to arbitrary locations outside the intended recovery directory via crafted filenames or directory paths with path traversal sequences in a filesystem image. An attacker can craft a malicious filesystem image with embedded /../ sequences in filenames that, when processed by tsk_recover, writes files outside the output directory, potentially achieving code execution by overwriting shell configuration or cron entries.	7.1	More Details
CVE-2026-33104	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32083	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32082	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32080	Use after free in Windows WalletService allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32195	Stack-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-33100	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32073	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32086	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32087	Heap-based buffer overflow in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32093	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-33099	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32224	Use after free in Windows Server Update Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-33018	libsixel is a SIXEL encoder/decoder implementation derived from kmiya's sixel. Versions 1.8.7 and prior contain a Use-After-Free vulnerability via the load_gif() function in fromgif.c, where a single sixel_frame_t object is reused across all frames of an animated GIF and gif_init_frame() unconditionally frees and reallocates frame->pixels between frames without consulting the object's reference count. Because the public API explicitly provides sixel_frame_ref() to retain a frame and sixel_frame_get_pixels() to access the raw pixel buffer, a callback following this documented usage pattern will hold a dangling pointer after the second frame is decoded, resulting in a heap use-after-free confirmed by ASAN. Any application using sixel_helper_load_image_file() with a multi-frame callback to process user-supplied animated GIFs is affected, with a reliable crash as the minimum impact and potential for code execution. This issue has been fixed in version 1.8.7-r1.	7.0	More Details
CVE-2026-39883	OpenTelemetry-Go is the Go implementation of OpenTelemetry. From 1.15.0 to 1.42.0, the fix for CVE-2026-24051 changed the Darwin ioreg command to use an absolute path but left the BSD kenv command using a bare name, allowing the same PATH hijacking attack on BSD and Solaris platforms. This vulnerability is fixed in 1.43.0.	7.0	More Details
CVE-2026-32150	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	7.0	More Details

CVE-2026-32219	Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32075	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-27921	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32070	Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-27908	Use after free in Windows TDI Translation Driver (tdx.sys) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-25184	Concurrent execution using shared resource with improper synchronization ('race condition') in Applocker Filter Driver (applockerfltr.sys) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26152	Insecure storage of sensitive information in Windows Cryptographic Services allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26165	Use after free in Windows Shell allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26166	Double free in Windows Shell allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26173	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26174	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Server Update Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26177	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-32068	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-26182	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-27917	Use after free in Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-27926	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-27929	Time-of-check time-of-use (toctou) race condition in Windows LUAFV allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-27922	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-28553	Vulnerability of improper permission control in the theme setting module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.9	More Details
	A flaw was found in Keycloak, specifically in the organization selection login page. A remote attacker with `manage-realm` or `manage-organizations` administrative privileges can exploit a Stored Cross-Site Scripting (XSS)		

CVE-2026-37980	vulnerability. This flaw occurs because the `organization.alias` is placed into an inline JavaScript `onclick` handler, allowing a crafted JavaScript payload to execute in a user's browser when they view the login page. Successful exploitation enables arbitrary JavaScript execution, potentially leading to session theft, unauthorized account actions, or further attacks against users of the affected realm.	6.9	More Details
CVE-2026-40446	Access of resource using incompatible type ('type confusion') vulnerability in Samsung Open Source Escargot allows Pointer Manipulation.This issue affects Escargot: 97e8115ab1110bc502b4b5e4a0c689a71520d335.	6.9	More Details
CVE-2026-21011	Incorrect privilege assignment in Bluetooth in Maintenance mode prior to SMR Apr-2026 Release 1 allows physical attackers to bypass Extend Unlock.	6.8	More Details
CVE-2026-35577	Apollo MCP Server is a Model Context Protocol server that exposes GraphQL operations as MCP tools. Prior to version 1.7.0, the Apollo MCP Server did not validate the Host header on incoming HTTP requests when using StreamableHTTP transport. In configurations where an HTTP-based MCP server is run on localhost without additional authentication or network-level controls, this could potentially allow a malicious website—visited by a user running the server locally—to use DNS rebinding techniques to bypass same-origin policy restrictions and issue requests to the local MCP server. If successfully exploited, this could allow an attacker to invoke tools or access resources exposed by the MCP server on behalf of the local user. This issue is limited to HTTP-based transport modes (StreamableHTTP). It does not affect servers using stdio transport. The practical risk is further reduced in deployments that use authentication, network-level access controls, or are not bound to localhost. This vulnerability is fixed in 1.7.0.	6.8	More Details
CVE-2025-15441	The Form Maker by 10Web WordPress plugin before 1.15.38 does not properly prepare SQL queries when the "MySQL Mapping" feature is in use, which could make SQL Injection attacks possible in certain contexts.	6.8	More Details
CVE-2026-32223	Heap-based buffer overflow in Windows USB Print Driver allows an unauthorized attacker to elevate privileges with a physical attack.	6.8	More Details
CVE-2025-31991	Rate Limiting for attempting a user login is not being properly enforced, making HCL DevOps Velocity susceptible to brute-force attacks past the unsuccessful login attempt limit. This vulnerability is fixed in 5.1.7.	6.8	More Details
CVE-2026-21007	Improper check for exceptional conditions in Device Care prior to SMR Apr-2026 Release 1 allows physical attackers to bypass Knox Guard.	6.8	More Details
CVE-2026-34864	Boundary-unlimited vulnerability in the application read module. Impact: Successful exploitation of this vulnerability may affect availability.	6.8	More Details
CVE-2026-5893	Race in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	6.8	More Details
CVE-2026-39961	Aiven Operator allows you to provision and manage Aiven Services from your Kubernetes cluster. From 0.31.0 to before 0.37.0, a developer with create permission on ClickhouseUser CRDs in their own namespace can exfiltrate secrets from any other namespace — production database credentials, API keys, service tokens — with a single kubectl apply. The operator reads the victim's secret using its ClusterRole and writes the password into a new secret in the attacker's namespace. The operator acts as a confused deputy: its ServiceAccount has cluster-wide secret read/write (aiven-operator-role ClusterRole), and it trusts user-supplied namespace values in spec.connInfoSecretSource.namespace without validation. No admission webhook enforces this boundary — the ServiceUser webhook returns nil, and no ClickhouseUser webhook exists. This vulnerability is fixed in 0.37.0.	6.8	More Details
CVE-2026-0390	Reliance on untrusted inputs in a security decision in Windows Boot Loader allows an authorized attacker to bypass a security feature locally.	6.7	More Details
CVE-2026-39814	A relative path traversal vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.1 through 7.4.12, FortiWeb 7.2.7 through 7.2.12, FortiWeb 7.0.10 through 7.0.12 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	6.7	More Details
CVE-2026-39809	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.0 through 7.4.5, FortiClientEMS 7.2.0 through 7.2.12, FortiClientEMS 7.0 all versions may allow attacker to execute unauthorized code or commands via sending crafted requests	6.7	More Details
CVE-2026-25691	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox Cloud 5.0.4, FortiSandbox PaaS 5.0.4 may allow a privileged attacker with super-admin profile and CLI access to delete an arbitrary directory via HTTP crafted requests.	6.7	More Details
CVE-2026-	A Permissive List of Allowed Input vulnerability in the CLI of Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows a local, high privileged attacker to escalate their privileges to root. The CLI menu accepts input without carefully validating it, which allows for shell command injection. These shell commands are executed	6.7	More

21915	with root permissions and can be used to gain complete control of the system. This issue affects all JSI vLWC versions before 3.0.94.		Details
CVE-2026-40224	In systemd 259 before 260, there is local privilege escalation in systemd-machined because varlink can be used to reach the root namespace.	6.7	More Details
CVE-2026-32176	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2026-32167	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2026-39389	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.4.0, This vulnerability is fixed in 0.31.4.0.	6.7	More Details
CVE-2025-30650	A Missing Authentication for Critical Function vulnerability in command processing of Juniper Networks Junos OS allows a privileged local attacker to gain access to Linux-based line cards as root. This issue affects systems running Junos OS using Linux-based line cards. Affected line cards include: * MPC7, MPC8, MPC9, MPC10, MPC11 * LC2101, LC2103 * LC480, LC4800, LC9600 * MX304 (built-in FPC) * MX-SPC3 * SRX5K-SPC3 * EX9200-40XS * FPC3-PTX-U2, FPC3-PTX-U3 * FPC3-SFF-PTX * LC1101, LC1102, LC1104, LC1105 This issue affects Junos OS: * all versions before 22.4R3-S8, * from 23.2 before 23.2R2-S6, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2, * from 25.2 before 25.2R2.	6.7	More Details
CVE-2026-4878	A flaw was found in libcap. A local unprivileged user can exploit a Time-of-check-to-time-of-use (TOCTOU) race condition in the `cap_set_file()` function. This allows an attacker with write access to a parent directory to redirect file capability updates to an attacker-controlled file. By doing so, capabilities can be injected into or stripped from unintended executables, leading to privilege escalation.	6.7	More Details
CVE-2026-35553	Bluetooth ACPI Drivers provided by Dynabook Inc. contain a stack-based buffer overflow vulnerability. An attacker may execute arbitrary code by modifying certain registry values.	6.7	More Details
CVE-2026-34863	Out-of-bounds write vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect availability.	6.7	More Details
CVE-2026-25206	Out-of-bounds read vulnerability in Samsung Open Source Escargot allows Resource Leak Exposure.This issue affects Escargot: 97e8115ab1110bc502b4b5e4a0c689a71520d335.	6.7	More Details
CVE-2026-33791	An OS Command Injection vulnerability in the CLI processing of Juniper Networks Junos OS and Junos OS Evolved allows a local, high-privileged attacker executing specific, crafted CLI commands to inject arbitrary shell commands as root, leading to a complete compromise of the system. Certain 'set system' commands, when executed with crafted arguments, are not properly sanitized, allowing for arbitrary shell injection. These shell commands are executed as root, potentially allowing for complete control of the vulnerable system. This issue affects: Junos OS: * all versions before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S7, * from 24.2 before 24.2R2-S2, * from 24.4 before 24.4R2, * from 25.2 before 25.2R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-S7-EVO, * from 24.2 before 24.2R2-S2-EVO, * from 24.4 before 24.4R2-EVO, * from 25.2 before 25.2R1-S1-EVO, 25.2R2-EVO.	6.7	More Details
CVE-2026-35479	InvenTree is an Open Source Inventory Management System. Prior to 1.2.7 and 1.3.0, any users who have staff access permissions can install plugins via the API, without requiring "superuser" account access. This level of permission requirement is out of alignment with other plugin actions (such as uninstalling) which do require superuser access. The vulnerability allows staff users (who may be considered to have a lower level of trust than a superuser account) to install arbitrary (and potentially harmful) plugins. This vulnerability is fixed in 1.2.7 and 1.3.0.	6.6	More Details
CVE-2026-27102	Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.1.6 and versions 9.11.0.0 through 9.13.0.1, contains an incorrect privilege assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	6.6	More Details
CVE-2026-4837	An eval() injection vulnerability in the Rapid7 Insight Agent beaconing logic for Linux versions could theoretically allow an attacker to achieve remote code execution as root via a crafted beacon response. Because the Agent uses mutual TLS (mTLS) to verify commands from the Rapid7 Platform, it is unlikely that the eval() function could be exploited remotely without prior, highly privileged access to the backend platform.	6.6	More Details
CVE-2026-20709	Use of Default Cryptographic Key in the hardware for some Intel(R) Pentium(R) Processor Silver Series, Intel(R) Celeron(R) Processor J Series, Intel(R) Celeron(R) Processor N Series may allow an escalation of privilege. Hardware reverse engineer adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via physical access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (high), integrity (high) and availability (none) impacts.	6.6	More Details

CVE-2026-5892	Insufficient policy enforcement in PWAs in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to install a PWA without user consent via a crafted HTML page. (Chromium security severity: Medium)	6.6	More Details
CVE-2026-21010	Improper input validation in Retail Mode prior to SMR Apr-2026 Release 1 allows local attackers to trigger privileged functions.	6.6	More Details
CVE-2026-5959	A security flaw has been discovered in GL.iNet GL-RM1, GL-RM10, GL-RM10RC and GL-RM1PE 1.8.1. Affected by this issue is some unknown functionality of the component Factory Reset Handler. Performing a manipulation results in improper authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 1.8.2 can 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.	6.6	More Details
CVE-2026-1865	The User Registration & Membership – Free & Paid Memberships, Subscriptions, Content Restriction, User Profile, Custom User Registration & Login Builder plugin for WordPress is vulnerable to SQL Injection via the 'membership_ids[]' parameter in all versions up to, and including, 5.1.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-39569	Missing Authorization vulnerability in AA Web Servant 12 Step Meeting List 12-step-meeting-list allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects 12 Step Meeting List: from n/a through <= 3.19.9.	6.5	More Details
CVE-2026-27677	Due to missing authorization checks in the SAP S/4HANA OData Service (Manage Reference Equipment), an attacker could update and delete child entities via OData services without proper authorization. This vulnerability has a high impact on integrity, while confidentiality and availability are not impacted.	6.5	More Details
CVE-2026-5207	The LifterLMS plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter in all versions up to, and including, 9.2.1. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Instructor-level access and above who have the edit_post capability on the quiz, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-25209	Out-of-bounds read vulnerability in Samsung Open Source Escargot allows Resource Leak Exposure.This issue affects Escargot: 97e8115ab1110bc502b4b5e4a0c689a71520d335.	6.5	More Details
CVE-2026-39575	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ronald Huereca Custom Query Blocks post-type-archive-mapping allows DOM-Based XSS.This issue affects Custom Query Blocks: from n/a through <= 5.5.0.	6.5	More Details
CVE-2026-27925	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an unauthorized attacker to disclose information over an adjacent network.	6.5	More Details
CVE-2026-34538	Apache Airflow versions 3.0.0 through 3.1.8 DagRun wait endpoint returns XCom result values even to users who only have DAG Run read permissions, such as the Viewer role.This behavior conflicts with the FAB RBAC model, which treats XCom as a separate protected resource, and with the security model documentation that defines the Viewer role as read-only. Airflow uses the FAB Auth Manager to manage access control on a per-resource basis. The Viewer role is intended to be read-only by default, and the security model documentation defines Viewer users as those who can inspect DAGs without accessing sensitive execution results. Users are recommended to upgrade to Apache Airflow 3.2.0 which resolves this issue.	6.5	More Details
CVE-2026-40039	Pachno 1.0.6 contains an open redirection vulnerability that allows attackers to redirect users to arbitrary external websites by manipulating the return_to parameter. Attackers can craft malicious login URLs with unvalidated return_to values to conduct phishing attacks and steal user credentials.	6.5	More Details
CVE-2026-27678	Due to missing authorization checks in the SAP S/4HANA backend OData Service (Manage Reference Structures), an attacker could update and delete child entities via exposed OData services without proper authorization. This vulnerability has a high impact on integrity, while confidentiality and availability are not impacted.	6.5	More Details
CVE-2025-14545	The YML for Yandex Market WordPress plugin before 5.0.26 is vulnerable to Remote Code Execution via the feed generation process.	6.5	More Details
CVE-2026-40043	Pachno 1.0.6 contains an authentication bypass vulnerability in the runSwitchUser() action that allows authenticated low-privilege users to escalate privileges by manipulating the original_username cookie. Attackers can set the client-controlled original_username cookie to any value and request a switch to user ID 1 to obtain session tokens or password hashes belonging to administrator accounts.	6.5	More Details
CVE-2026-4432	The YITH WooCommerce Wishlist WordPress plugin before 4.13.0 does not properly validate wishlist ownership in the save_title() AJAX handler before allowing wishlist renaming operations. The function only checks for a valid nonce, which is publicly exposed in the page source of the /wishlist/ page, making it possible for unauthenticated attackers to rename any wishlist belonging to any user on the site.	6.5	More Details

CVE-2026-40199	Net::CIDR::Lite versions before 0.23 for Perl mishandles IPv4 mapped IPv6 addresses, which may allow IP ACL bypass. _pack_ipv6() includes the sentinel byte from _pack_ipv4() when building the packed representation of IPv4 mapped addresses like ::ffff:192.168.1.1. This produces an 18 byte value instead of 17 bytes, misaligning the IPv4 part of the address. The wrong length causes incorrect results in mask operations (bitwise AND truncates to the shorter operand) and in find() / bin_find() which use Perl string comparison (lt/gt). This can cause find() to incorrectly match or miss addresses. Example: my $cidr = Net::CIDR::Lite->new("::ffff:192.168.1.0/120"); $cidr->find("::ffff:192.168.2.0"); # incorrectly returns true This is triggered by valid RFC 4291 IPv4 mapped addresses (::ffff:x.x.x.x). See also CVE-2026-40198, a related issue in the same function affecting malformed IPv6 addresses.	6.5	More Details
CVE-2026-34370	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, the notebook module contains an Insecure Direct Object Reference (IDOR) vulnerability that allows any authenticated student to read the private course notes of any other user on the platform by manipulating the notebook_id parameter in the editnote action. The application fetches the note content using only the supplied integer ID without verifying that the requesting user owns the note, and the full title and HTML body are rendered in the edit form and returned to the attacker's browser. While ownership checks exist in the write paths (updateNote() and delete_note()), they are entirely absent from the read path (get_note_information()). This issue has been fixed in version 2.0.0-RC.3.	6.5	More Details
CVE-2026-2377	A flaw was found in mirror-registry. Authenticated users can exploit the log export feature by providing a specially crafted web address (URL). This allows the application's backend to make arbitrary requests to internal network resources, a vulnerability known as Server-Side Request Forgery (SSRF). This could lead to unauthorized access to sensitive information or other internal systems.	6.5	More Details
CVE-2026-5919	Insufficient validation of untrusted input in WebSockets in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-40148	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the _safe_extractall() function in PraisonAI's recipe registry validates archive members against path traversal attacks but performs no checks on individual member sizes, cumulative extracted size, or member count before calling tar.extractall(). An attacker can publish a malicious recipe bundle containing highly compressible data (e.g., 10GB of zeros compressing to ~10MB) that exhausts the victim's disk when pulled via LocalRegistry.pull() or HttpRegistry.pull(). This vulnerability is fixed in 4.5.128.	6.5	More Details
CVE-2026-27679	Due to missing authorization checks in the SAP S/4HANA frontend OData Service (Manage Reference Structures), an attacker could update and delete child entities via exposed OData services without proper authorization. This vulnerability has a high impact on integrity, while confidentiality and availability are not impacted.	6.5	More Details
CVE-2026-23900	Various stored XSS vulnerabilities in the maps- and icon rendering logic in Phoca Maps component 5.0.0-6.0.2 have been discovered.	6.5	More Details
CVE-2026-40037	OpenClaw before 2026.3.31 (patched in 2026.4.8) contains a request body replay vulnerability in fetchWithSsrFGuard that allows unsafe request bodies to be resent across cross-origin redirects. Attackers can exploit this by triggering redirects to exfiltrate sensitive request data or headers to unintended origins.	6.5	More Details
CVE-2026-39943	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 11.17.0, Directus stores revision records (in directus_revisions) whenever items are created or updated. Due to the revision snapshot code not consistently calling the prepareDelta sanitization pipeline, sensitive fields (including user tokens, two-factor authentication secrets, external auth identifiers, auth data, stored credentials, and AI provider API keys) could be stored in plaintext within revision records. This vulnerability is fixed in 11.17.0.	6.5	More Details
CVE-2026-34261	Due to a missing authorization check in SAP Business Analytics and SAP Content Management, an authenticated user could make unauthorized calls to certain remote function modules, potentially accessing sensitive information beyond their intended permissions. This vulnerability affects confidentiality, with no impact on integrity and availability.	6.5	More Details
CVE-2026-39632	Cross-Site Request Forgery (CSRF) vulnerability in ThemeGoods Grand Blog grandblog allows Cross Site Request Forgery.This issue affects Grand Blog: from n/a through <= 3.1.	6.5	More Details
CVE-2026-34264	During authorization checks in SAP Human Capital Management for SAP S/4HANA, the system returns specific messages. Due to this, an authenticated user with low privileges could guess and enumerate the content shown, beyond their authorized scope. This leads to disclosure of sensitive information causing a high impact on confidentiality, while integrity and availability are unaffected.	6.5	More Details
CVE-2026-39633	Cross-Site Request Forgery (CSRF) vulnerability in ThemeGoods Grand Car Rental grandcarrental allows Cross Site Request Forgery.This issue affects Grand Car Rental: from n/a through <= 3.6.9.	6.5	More Details
CVE-2025-3756	A vulnerability exists in the command handling of the IEC 61850 communication stack included in the product revisions listed as affected in this CVE. An attacker with access to IEC 61850 networks could exploit the vulnera bility by using a specially crafted 61850 packet, forcing the communication interfaces of the PM 877, CI850 and CI868 modules into fault mode or causing unavailability of the S+ Operations 61850 connectivity, resulting in a denial-of-service situation. The System 800xA IEC61850 Connect is not affected. Note: This vulnerability does not impact on the overall availability and functionality of the S+ Operations node, only the 61850 communication function. This issue affects AC800M (System 800xA): from 6.0.0x through 6.0.0303.0, from 6.1.0x through 6.1.0031.0, from 6.1.1x through 6.1.1004.0, from 6.1.1x through 6.1.1202.0, from 6.2.0x through 6.2.0006.0; Symphony Plus SD Series: A_0, A_1, A_2.003, A_3.005, A_4.001, B_0.005; Symphony Plus MR (Melody Rack): from 3.10 through 3.52; S+ Operations: 2.1, 2.2, 2.3, 3.3.	6.5	More Details

CVE-2026-26155	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	6.5	More Details
CVE-2025-53847	A missing authentication for critical function vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiOS 6.4 all versions, FortiOS 6.2.9 through 6.2.17 allows attacker to execute unauthorized code or commands via specially crafted packets.	6.5	More Details
CVE-2026-39646	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bozdoz Leaflet Map leaflet-map allows Stored XSS.This issue affects Leaflet Map: from n/a through <= 3.4.4.	6.5	More Details
CVE-2026-5876	Side-channel information leakage in Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-33736	Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, any authenticated user (including ROLE_STUDENT) can enumerate all platform users and access personal information (email, phone, roles) via GET /api/users, including administrator accounts. This vulnerability is fixed in 2.0.0-RC.3.	6.5	More Details
CVE-2026-33459	Uncontrolled Resource Consumption (CWE-400) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user with access to the automatic import feature can submit specially crafted requests with excessively large input values. When multiple such requests are sent concurrently, the backend services become unstable, resulting in service disruption and deployment unavailability for all users.	6.5	More Details
CVE-2026-33708	Chamilo LMS is a learning management system. Prior to 1.11.38, the get_user_info_from_username REST API endpoint returns personal information (email, first name, last name, user ID, active status) of any user to any authenticated user, including students. There is no authorization check. This vulnerability is fixed in 1.11.38.	6.5	More Details
CVE-2026-21008	Exposure of sensitive information in S Share prior to SMR Apr-2026 Release 1 allows adjacent attacker to access sensitive information.	6.5	More Details
CVE-2026-35621	OpenClaw before 2026.3.24 contains a privilege escalation vulnerability where the /allowlist command fails to re-validate gateway client scopes for internal callers, allowing operator.write-scoped clients to mutate channel authorization policy. Attackers can exploit chat.send to build an internal command-authorized context and persist channel allowFrom and groupAllowFrom policy changes reserved for operator.admin scope.	6.5	More Details
CVE-2026-39708	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uicore UiCore Elements uicore-elements allows Stored XSS.This issue affects UiCore Elements: from n/a through <= 1.3.14.	6.5	More Details
CVE-2026-35649	OpenClaw before 2026.3.22 contains a settings reconciliation vulnerability that allows attackers to bypass intended deny-all revocations by exploiting empty allowlist handling. The vulnerability treats explicit empty allowlists as unset during reconciliation, silently undoing intended access control denials and restoring previously revoked permissions.	6.5	More Details
CVE-2026-35652	OpenClaw before 2026.3.22 contains an authorization bypass vulnerability in interactive callback dispatch that allows non-allowlisted senders to execute action handlers. Attackers can bypass sender authorization checks by dispatching callbacks before normal security validation completes, enabling unauthorized actions.	6.5	More Details
CVE-2026-35599	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the addRepeatIntervalToTime function uses an O(n) loop that advances a date by the task's RepeatAfter duration until it exceeds the current time. By creating a repeating task with a 1-second interval and a due date far in the past, an attacker triggers billions of loop iterations, consuming CPU and holding a database connection for minutes per request. This vulnerability is fixed in 2.3.0.	6.5	More Details
CVE-2026-35656	OpenClaw before 2026.3.22 contains an authentication bypass vulnerability in the X-Forwarded-For header processing when trustedProxies is configured, allowing attackers to spoof loopback hops. Remote attackers can inject forged forwarding headers to bypass canvas authentication and rate-limiting protections by masquerading as loopback clients.	6.5	More Details
CVE-2026-35657	OpenClaw before 2026.3.25 contains an authorization bypass vulnerability in the HTTP /sessions/:sessionKey/history route that skips operator.read scope validation. Attackers can access session history without proper operator read permissions by sending HTTP requests to the vulnerable endpoint.	6.5	More Details
CVE-2026-35658	OpenClaw before 2026.3.2 contains a filesystem boundary bypass vulnerability in the image tool that fails to honor tools.fs.workspaceOnly restrictions. Attackers can traverse sandbox bridge mounts outside the workspace to read files that other filesystem tools would reject.	6.5	More Details
CVE-2026-35403	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 15.10 to before 27.0.3 and 28.0.1, there is a potential for a cross-site scripting attack in the survey_accounts module if a user provides an invalid visit label. While the data is properly JSON encoded, the Content-Type header is not set causing the web browser to interpret the payload as HTML, opening the possibility of a cross-site scripting if a user is tricked into following an invalid link. This vulnerability is fixed in 27.0.3 and 28.0.1.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elfsight Elfsight		

2026-39696	WhatsApp Chat CC elfsight-whatsapp-chat allows DOM-Based XSS.This issue affects Elfsight WhatsApp Chat CC: from n/a through <= 1.2.0.	6.5	More Details
CVE-2026-35034	Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a denial of service vulnerability in the SyncPlay group creation endpoint (POST /SyncPlay/New), where an authenticated user can create groups with names of unlimited size due to insufficient input validation. By sending large payloads combined with arbitrary group IDs, an attacker can lock out the endpoint for other clients attempting to join SyncPlay groups and significantly increase the memory usage of the Jellyfin process, potentially leading to an out-of-memory crash. This issue has been fixed in version 10.11.7.	6.5	More Details
CVE-2026-35594	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, Vikunja's link share authentication (GetLinkShareFromClaims in pkg/models/link_sharing.go) constructs authorization objects entirely from JWT claims without any server-side database validation. When a project owner deletes a link share or downgrades its permissions, all previously issued JWTs continue to grant the original permission level for up to 72 hours (the default service.jwtttl). This vulnerability is fixed in 2.3.0.	6.5	More Details
CVE-2026-35407	Saleor is an e-commerce platform. From 2.10.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, a business-logic and authorization flaw was found in the account email change workflow, the confirmation flow did not verify that the email change confirmation token was issued for the given authenticated user. As a result, a valid email-change token generated for one account can be replayed while authenticated as a different account. The second account’s email address is then updated to the token's new_email, even though that token was never issued for that account. This vulnerability is fixed in 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118.	6.5	More Details
CVE-2026-22155	A cleartext transmission of sensitive information vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow attacker to information disclosure via <insert attack vector here>	6.5	More Details
CVE-2026-39508	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Josh Kohlbach Advanced Coupons for WooCommerce Coupons advanced-coupons-for-woocommerce-free allows DOM-Based XSS.This issue affects Advanced Coupons for WooCommerce Coupons: from n/a through <= 4.7.1.1.	6.5	More Details
CVE-2026-39483	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hidekazu Ishikawa VK All in One Expansion Unit vk-all-in-one-expansion-unit allows Stored XSS.This issue affects VK All in One Expansion Unit: from n/a through <= 9.113.3.	6.5	More Details
CVE-2026-39517	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in A WP Life Blog Filter blog-filter allows DOM-Based XSS.This issue affects Blog Filter: from n/a through <= 1.7.6.	6.5	More Details
CVE-2026-22573	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5 all versions, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5 all versions, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to perform path traversal attack via File Content Extraction actions.	6.5	More Details
CVE-2026-39482	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PublishPress Post Expirator post-expirator allows DOM-Based XSS.This issue affects Post Expirator: from n/a through <= 4.9.4.	6.5	More Details
CVE-2026-39641	Cross-Site Request Forgery (CSRF) vulnerability in Skywarrior Blackfyre blackfyre allows Cross Site Request Forgery.This issue affects Blackfyre: from n/a through <= 2.5.4.	6.5	More Details
CVE-2026-34500	CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled and FFM is used in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M14 through 11.0.20, from 10.1.22 through 10.1.53, from 9.0.92 through 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fixes the issue.	6.5	More Details
CVE-2026-6068	NASM contains a heap use after free vulnerability in response file (-@) processing where a dangling pointer to freed memory is stored in the global depend_file and later dereferenced, as the response-file buffer is freed before the pointer is used, allowing for data corruption or unexpected behavior.	6.5	More Details
CVE-2026-32151	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-1101	GitLab has remediated an issue in GitLab EE affecting all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user to cause denial of service to the GitLab instance due to improper input validation in GraphQL queries.	6.5	More Details
CVE-2026-33141	Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the REST API stats endpoint allows any authenticated user (including low-privilege students with ROLE_USER) to read any other user's learning progress, certificates, and gradebook scores for any course, without enrollment or supervisory relationship. This vulnerability is fixed in 2.0.0-RC.3.	6.5	More Details
CVE-			

2026-32201	Improper input validation in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-39674	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Manoj Kumar MK Google Directions google-distance-calculator allows DOM-Based XSS.This issue affects MK Google Directions: from n/a through <= 3.1.1.	6.5	More Details
CVE-2026-27460	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.6.5, a critical Denial of Service (DoS) vulnerability was in the recipe import functionality. This vulnerability allows an authenticated user to crash the server or make a significantly degrade its performance by uploading a large size ZIP file (ZIP Bomb). This vulnerability is fixed in 2.6.5.	6.5	More Details
CVE-2021-47960	A files or directories accessible to external parties vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access files within the installation directory via a local HTTP server bound to the loopback interface. By leveraging user interaction with a crafted web page, attackers may retrieve sensitive files such as configuration files, certificates, and logs, leading to information disclosure.	6.5	More Details
CVE-2026-39636	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in livemesh Livemesh Addons for Elementor addons-for-elementor allows Stored XSS.This issue affects Livemesh Addons for Elementor: from n/a through <= 9.0.	6.5	More Details
CVE-2026-39500	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themesflat themesflat-addons-for-elementor themesflat-addons-for-elementor allows Stored XSS.This issue affects themesflat-addons-for-elementor: from n/a through <= 2.3.2.	6.5	More Details
CVE-2026-33781	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX and QFX Series devices allow an unauthenticated, adjacent attacker to cause a complete Denial of Service (DoS). On EX4k, and QFX5k platforms configured as service-provider edge devices, if L2PT is enabled on the UNI and VSTP is enabled on NNI in VXLAN scenarios, receiving VSTP BPDUs on UNI leads to packet buffer allocation failures, resulting in the device to not pass traffic anymore until it is manually recovered with a restart.This issue affects Junos OS: * 24.4 releases before 24.4R2, * 25.2 releases before 25.2R1-S1, 25.2R2. This issue does not affect Junos OS releases before 24.4R1.	6.5	More Details
CVE-2026-35644	OpenClaw before 2026.3.22 contains an information disclosure vulnerability that allows attackers with operator.read scope to expose credentials embedded in channel baseUrl and httpUrl fields. Attackers can access gateway snapshots via config.get and channels.status endpoints to retrieve sensitive authentication information from URL userinfo components.	6.5	More Details
CVE-2026-3480	The WP Blockade plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 0.9.14. The plugin registers an admin_post action hook 'wp-blockade-shortcode-render' that maps to the render_shortcode_preview() function. This function lacks any capability check (current_user_can()) and nonce verification, allowing any authenticated user to execute arbitrary WordPress shortcodes. The function takes a user-supplied 'shortcode' parameter from $_GET, passes it through stripslashes(), and directly executes it via do_shortcode(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes, which could lead to information disclosure, privilege escalation, or other impacts depending on what shortcodes are registered on the site (e.g., shortcodes from other plugins that display sensitive data, perform actions, or include files).	6.5	More Details
CVE-2026-33779	An Improper Following of a Certificate's Chain of Trust vulnerability in J-Web of Juniper Networks Junos OS on SRX Series allows a PITM to intercept the communication of the device and get access to confidential information and potentially modify it. When an SRX device is provisioned to connect to Security Director (SD) cloud, it doesn't perform sufficient verification of the received server certificate. This allows a PITM to intercept the communication between the SRX and SD cloud and access credentials and other sensitive information. This issue affects Junos OS: * all versions before 22.4R3-S9, * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R1-S2, 25.2R2.	6.5	More Details
CVE-2026-33780	A Missing Release of Memory after Effective Lifetime vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker to cause a memory leak ultimately leading to a Denial of Service (DoS). In an EVPN-MPLS scenario, routes learned from remote multi-homed Provider Edge (PE) devices are programmed as ESI routes. Due to a logic issue in the l2ald memory management, memory allocated for these routes is not released when there is churn for these routes. As a result, memory leaks in the l2ald process which will ultimately lead to a crash and restart of l2ald. Use the following command to monitor the memory consumption by l2ald: user@device> show system process extensive | match "PID|l2ald" This issue affects: Junos OS: * all versions before 22.4R3-S5, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2; Junos OS Evolved: * all versions before 22.4R3-S5-EVO, * 23.2 versions before 23.2R2-S3-EVO, * 23.4 versions before 23.4R2-S4-EVO, * 24.2 versions before 24.2R2-EVO.	6.5	More Details
CVE-2026-5888	Uninitialized Use in WebCodecs in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-35636	OpenClaw versions 2026.3.11 through 2026.3.24 contain a session isolation bypass vulnerability where session_status resolves sessionId to canonical session keys before enforcing visibility checks. Sandboxed child sessions can exploit this to access parent or sibling sessions that should be blocked by explicit sessionKey restrictions.	6.5	More Details

CVE-2025-59969	A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the advanced forwarding toolkit (evo-aftmand/evo-pfemand) of Juniper Networks Junos OS Evolved on PTX Series or QFX5000 Series allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS).An attacker sending crafted multicast packets will cause line cards running evo-aftmand/evo-pfemand to crash and restart or non-line card devices to crash and restart. Continued receipt and processing of these packets will sustain the Denial of Service (DoS) condition. This issue affects Junos OS Evolved PTX Series: * All versions before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-EVO, * from 24.2 before 24.2R2-EVO, * from 24.4 before 24.4R2-EVO. This issue affects Junos OS Evolved on QFX5000 Series: * 22.2-EVO version before 22.2R3-S7-EVO, * 22.4-EVO version before 22.4R3-S7-EVO, * 23.2-EVO versions before 23.2R2-S4-EVO, * 23.4-EVO versions before 23.4R2-S5-EVO, * 24.2-EVO versions before 24.2R2-S1-EVO, * 24.4-EVO versions before 24.4R1-S3-EVO, 24.4R2-EVO. This issue does not affect Junos OS Evolved on QFX5000 Series versions before: 21.2R2-S1-EVO, 21.2R3-EVO, 21.3R2-EVO, 21.4R1-EVO, and 22.1R1-EVO.	6.5	More Details
CVE-2026-33782	A Missing Release of Memory after Effective Lifetime vulnerability in the DHCP daemon (jdhcpd) of Juniper Networks Junos OS on MX Series, allows an adjacent, unauthenticated attacker to cause a memory leak, that will eventually cause a complete Denial-of-Service (DoS). In a DHCPv6 over PPPoE, or DHCPv6 over VLAN with Active lease query or Bulk lease query scenario, every subscriber logout will leak a small amount of memory. When all available memory has been exhausted, jdhcpd will crash and restart which causes a complete service impact until the process has recovered. The memory usage of jdhcpd can be monitored with: user@host> show system processes extensive | match jdhcpd This issue affects Junos OS: * all versions before 22.4R3-S1, * 23.2 versions before 23.2R2, * 23.4 versions before 23.4R2.	6.5	More Details
CVE-2026-35631	OpenClaw before 2026.3.22 fails to enforce operator.admin scope on mutating internal ACP chat commands, allowing unauthorized modifications. Attackers without admin privileges can execute mutating control-plane actions by directly invoking affected ACP commands to bypass authorization gates.	6.5	More Details
CVE-2026-33783	A Function Call With Incorrect Argument Type vulnerability in the sensor interface of Juniper Networks Junos OS Evolved on PTX Series allows a network-based, authenticated attacker with low privileges to cause a complete Denial of Service (DoS). If colored SRTE policy tunnels are provisioned via PCEP, and gRPC is used to monitor traffic in these tunnels, evo-aftmand crashes and doesn't restart which leads to a complete and persistent service impact. The system has to be manually restarted to recover. The issue is seen only when the Originator ASN field in PCEP contains a value larger than 65,535 (32-bit ASN). The issue is not reproducible when SRTE policy tunnels are statically configured. This issue affects Junos OS Evolved on PTX Series: * all versions before 22.4R3-S9-EVO, * 23.2 versions before 23.2R2-S6-EVO, * 23.4 versions before 23.4R2-S7-EVO, * 24.2 versions before 24.2R2-S4-EVO, * 24.4 versions before 24.4R2-S2-EVO, * 25.2 versions before 25.2R1-S2-EVO, 25.2R2-EVO.	6.5	More Details
CVE-2026-39692	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer allows Stored XSS.This issue affects tagDiv Composer: from n/a through <= 5.4.3.	6.5	More Details
CVE-2026-39639	Missing Authorization vulnerability in redpixelstudios RPS Include Content rps-include-content allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RPS Include Content: from n/a through <= 1.2.2.	6.5	More Details
CVE-2026-35627	OpenClaw before 2026.3.22 performs cryptographic and dispatch operations on inbound Nostr direct messages before enforcing sender and pairing policy validation. Attackers can trigger unauthorized pre-authentication computation by sending crafted DM messages, enabling denial of service through resource exhaustion.	6.5	More Details
CVE-2026-2582	The The Germanized for WooCommerce plugin for WordPress is vulnerable to arbitrary shortcode execution via 'account_holder' parameter in all versions up to, and including, 3.20.5. 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-2026-5881	Policy bypass in LocalNetworkAccess in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-35618	OpenClaw before 2026.3.23 contains a replay identity vulnerability in Plivo V2 signature verification that allows attackers to bypass replay protection by modifying query parameters. The verification path derives replay keys from the full URL including query strings instead of the canonicalized base URL, enabling attackers to mint new verified request keys through unsigned query-only changes to signed requests.	6.5	More Details
CVE-2026-1672	The BEAR – Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.5. This is due to missing nonce validation on the woobe_redraw_table_row() function. This makes it possible for unauthenticated attackers to update WooCommerce product data including prices, descriptions, and other product fields via a forged request granted they can trick a site administrator or shop manager into performing an action such as clicking on a link.	6.5	More Details
CVE-2026-5903	Policy bypass in IFrameSandbox in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-39703	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpbits WPBITS Addons For Elementor Page Builder wpbits-addons-for-elementor allows Stored XSS.This issue affects WPBITS Addons For Elementor Page Builder: from n/a through <= 1.8.1.	6.5	More Details
CVE-	Insufficient policy enforcement in DevTools in Google Chrome prior to 147.0.7727.55 allowed an attacker who		

2026-5901	convinced a user to install a malicious extension to bypass enterprise host restrictions for cookie modification via a crafted Chrome Extension. (Chromium security severity: Low)	6.5	More Details
CVE-2026-5885	Insufficient validation of untrusted input in WebML in Google Chrome on Windows prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2026-39848	Dockyard is a Docker container management app. Prior to 1.1.0, Docker container start and stop operations are performed through GET requests without CSRF protection. A remote attacker can cause a logged-in administrator's browser to request /apps/action.php?action=stop&name=<container> or /apps/action.php?action=start&name=<container>, which starts or stops the target container. This vulnerability is fixed in 1.1.0.	6.5	More Details
CVE-2026-33774	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass the configured firewall filter and access the control-plane of the device. On MX platforms with MPC10, MPC11, LC4800 or LC9600 line cards, and MX304, firewall filters applied on a loopback interface lo0.n (where n is a non-0 number) don't get executed when lo0.n is in the global VRF / default routing-instance. An affected configuration would be: user@host# show configuration interfaces lo0 | display set set interfaces lo0 unit 1 family inet filter input <filter-name> where a firewall filter is applied to a non-0 loopback interface, but that loopback interface is not referred to in any routing-instance (RI) configuration, which implies that it's used in the default RI. The issue can be observed with the CLI command: user@device> show firewall counter filter <filter_name> not showing any matches. This issue affects Junos OS on MX Series: * all versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2, * 24.4 versions before 24.4R2.	6.5	More Details
CVE-2026-39702	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wealcoder Animation Addons for Elementor animation-addons-for-elementor allows DOM-Based XSS.This issue affects Animation Addons for Elementor: from n/a through <= 2.6.1.	6.5	More Details
CVE-2026-33775	A Missing Release of Memory after Effective Lifetime vulnerability in the BroadBand Edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). If the authentication packet-type option is configured and a received packet does not match that packet type, the memory leak occurs. When all memory available to bbe-smgd has been consumed, no new subscribers will be able to login. The memory utilization of bbe-smgd can be monitored with the following show command: user@host> show system processes extensive | match bbe-smgd The below log message can be observed when this limit has been reached: bbesmgd[<PID>]: %DAEMON-3-SMD_DPROF_RSMON_ERROR: Resource unavailability, Reason: Daemon Heap Memory exhaustion This issue affects Junos OS on MX Series: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R2.	6.5	More Details
CVE-2026-5905	Incorrect security UI in Permissions in Google Chrome on Windows prior to 147.0.7727.55 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2026-39666	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in telepathy Hello Bar Popup Builder hellobar allows DOM-Based XSS.This issue affects Hello Bar Popup Builder: from n/a through <= 1.5.1.	6.5	More Details
CVE-2026-21919	An Incorrect Synchronization vulnerability in the management daemon (mgd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based attacker with low privileges to cause a complete Denial-of-Service (DoS) of the management plane. When NETCONF sessions are quickly established and disconnected, a locking issue causes mgd processes to hang in an unusable state. When the maximum number of mgd processes has been reached, no new logins are possible. This leads to the inability to manage the device and requires a power-cycle to recover. This issue can be monitored by checking for mgd processes in lockf state in the output of 'show system processes extensive': user@host> show system processes extensive | match mgd <pid> root 20 0 501M 4640K lockf 1 0:01 0.00% mgd If the system still can be accessed (either via the CLI or as root, which might still be possible as last resort as this won't invoke mgd), mgd processes in this state can be killed with 'request system process terminate <PID>' from the CLI or with 'kill -9 <PID>' from the shell. This issue affects: Junos OS: * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2-S1, * 24.4 versions before 24.4R1-S3, 24.4R2; This issue does not affect Junos OS versions before 23.4R1; Junos OS Evolved: * 23.4 versions before 23.4R2-S5-EVO, * 24.2 versions before 24.2R2-S1-EVO, * 24.4 versions before 24.4R1-S3-EVO, 24.4R2-EVO. This issue does not affect Junos OS Evolved versions before 23.4R1-EVO;	6.5	More Details
CVE-2026-39665	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vladimir Prelovac SEO Friendly Images seo-image allows DOM-Based XSS.This issue affects SEO Friendly Images: from n/a through <= 3.0.5.	6.5	More Details
CVE-2026-3513	The TableOn – WordPress Posts Table Filterable plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tableon_button' shortcode in all versions up to and including 1.0.4.4. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes such as 'class', 'help_link', 'popup_title', and 'help_title'. The do_shortcode_button() function extracts these attributes without sanitization and passes them to TABLEON_HELPER::draw_html_item(), which concatenates attribute values into HTML using single quotes without escaping (line 29: $item .= " {$key}='{$value}'"). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-57851	A container privilege escalation flaw was found in certain Multicluster Engine for Kubernetes images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	6.4	More Details
CVE-2026-3005	The List category posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catlist' shortcode in all versions up to, and including, 0.94.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4785	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_caption' parameter in the [latepoint_resources] shortcode in versions up to and including 5.3.0. This is due to insufficient output escaping when the 'items' parameter is set to 'bundles'. 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-2026-3618	The Columns by BestWebSoft plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' shortcode attribute of the [print_clmns] shortcode in all versions up to and including 1.0.3. This is due to insufficient input sanitization and output escaping on the 'id' attribute. The shortcode receives the 'id' parameter via shortcode_atts() at line 596 and directly embeds it into HTML output at line 731 (in a div id attribute) and into inline CSS at lines 672-729 without any escaping or sanitization. While the SQL query uses %d to cast the value to an integer for database lookup, the original unsanitized string value of $id is still used in the HTML/CSS output. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The attack requires that at least one column exists in the plugin (created by an admin), as the SQL query must return results for the output branch to be reached.	6.4	More Details
CVE-2026-4303	The WP Visitor Statistics (Real Time Traffic) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wsm_showDayStatsGraph' shortcode in all versions up to, and including, 8.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-40226	In nspawn in systemd 233 through 259 before 260, an escape-to-host action can occur via a crafted optional config file.	6.4	More Details
CVE-2026-3311	The The Plus Addons for Elementor – Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Progress Bar shortcode in all versions up to, and including, 6.4.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5451	The Extensions for Leaflet Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'elevation-track' shortcode in all versions up to, and including, 4.14. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5357	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sid' parameter of the 'wpdm_members' shortcode in versions up to and including 3.3.52. This is due to insufficient input sanitization and output escaping on the user-supplied 'sid' shortcode attribute. The sid parameter is extracted without sanitization in the members() function and stored via update_post_meta(), then echoed directly into an HTML id attribute in the members.php template without applying esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.	6.4	More Details
CVE-2026-2509	The Page Builder: Pagelayer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Button widget's Custom Attributes field in all versions up to, and including, 2.0.8. This is due to an incomplete event handler blocklist in the 'pagelayer_xss_content' XSS filtering function, which blocks common, but not all, event handlers. 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-2026-4333	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'skin' attribute of the learn_press_courses shortcode in all versions up to and including 4.3.3. This is due to insufficient input sanitization and output escaping on the 'skin' shortcode attribute. The attribute value is used directly in an sprintf() call that generates HTML (class attribute and data-layout attribute) without any esc_attr() 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-2026-3600	The Investi plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'investi-announcements-accordion' shortcode's 'maximum-num-years' attribute in all versions up to, and including, 1.0.26. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, the 'maximum-num-years' attribute value is read directly from shortcode attributes and interpolated into a double-quoted HTML attribute without any escaping (no esc_attr(), htmlspecialchars(), or similar). 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-2026-4300	The Robo Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Loading Label' setting in all versions up to, and including, 5.1.3. The plugin uses a custom `|***...***|` marker pattern in its `fixJsFunction()` method to embed raw JavaScript function references within JSON-encoded configuration objects. When a gallery's options are rendered on the frontend, `json_encode()` wraps all string values in double quotes. The `fixJsFunction()` method then strips the `"|***` and `***|"` sequences, effectively converting a JSON string value into raw JavaScript code. The Loading Label field (stored as `rbs_gallery_LoadingWord` post_meta) is an `rbstext` type field that is sanitized with `sanitize_text_field()` on save. While this strips HTML tags, it does not strip the `|***...***|` markers since they contain no HTML. When a user inputs `|***alert(document.domain)***|`, the value passes through sanitization intact, is stored in post_meta, and is later retrieved and output within an inline `<script>` tag via `renderMainBlock()` with the quote markers stripped — resulting in arbitrary JavaScript execution. The gallery post type uses `capability_type => 'post'`, allowing Author-level users to create galleries. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses a page containing the gallery shortcode.	6.4	More Details
CVE-2025-58713	A container privilege escalation flaw was found in certain Red Hat Process Automation Manager images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	6.4	More Details
CVE-2026-3498	The BlockArt Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'clientId' block attribute in all versions up to, and including, 2.2.15. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-57854	A container privilege escalation flaw was found in certain OpenShift Update Service (OSUS) images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, may be able to leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	6.4	More Details
CVE-2026-2988	The Blubrry PowerPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'powerpress' and 'podcast' shortcodes in versions up to, and including, 11.15.15 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-2026-4341	The Prime Slider – Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'follow_us_text' setting of the Mount widget in all versions up to, and including, 4.1.10. This is due to insufficient input sanitization and output escaping. Specifically, the `render_social_link()` function in `modules/mount/widgets/mount.php` outputs the `follow_us_text` Elementor widget setting using `echo` without any escaping function. The setting value is stored in `_elementor_data` post meta via `update_post_meta`. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-32282	On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.	6.4	More Details
CVE-2026-3239	The Strong Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's testimonial_view shortcode in all versions up to, and including, 3.2.21 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-40225	In udev in systemd before 260, local root execution can occur via malicious hardware devices and unsanitized kernel output.	6.4	More Details
CVE-2026-1396	The Magic Conversation For Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'magic-conversation' shortcode in all versions up to, and including, 3.0.97 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4895	The GreenShift - Animation and Page Builder Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 12.8.9 This is due to insufficient input sanitization and output escaping in the gspb_greenShift_block_script_assets() function. The function uses str_replace() to insert 'fetchpriority="high"' before 'src=' attributes when processing greenshift-blocks/image blocks with the disablelazy attribute enabled. Because this replacement operates on the entire HTML string without parsing, contributors can inject the string 'src=' into HTML attribute values (such as class attributes). When the str_replace executes, the double quotes in the replacement string break out of the attribute context, allowing injection of malicious HTML attributes like onfocus with JavaScript payloads. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
	The Surbma | Booking.com Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's		

CVE-2026-1607	`surbma-bookingcom` shortcode in all versions up to, and including, 2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5506	The Wavr plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `wave` shortcode in all versions up to, and including, 0.2.6. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5508	The WowPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `wowpress` shortcode in all versions up to, and including, 1.0.0. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4336	The Ultimate FAQ Accordion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via FAQ content in all versions up to, and including, 2.4.7. This is due to the plugin calling html_entity_decode() on post_content during rendering in the set_display_variables() function (View.FAQ.class.php, line 746), which converts HTML entity-encoded payloads back into executable HTML, combined with insufficient output escaping in the faq-answer.php template where the decoded content is echoed without wp_kses_post() or any other sanitization. The ufaq custom post type is registered with 'show_in_rest' => true and defaults to 'post' capability_type, allowing Author-level users to create and publish FAQs via the REST API. An Author can submit entity-encoded malicious HTML (e.g., <img src=x onerror=alert()>) which bypasses WordPress's kses sanitization at save time (since kses sees entities as plain text, not tags), but is then decoded back into executable HTML by html_entity_decode() at render time. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in FAQ pages that will execute whenever a user accesses an injected FAQ, either directly or via the [ultimate-faqs] shortcode.	6.4	More Details
CVE-2026-4073	The pdfl.io plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pdflio' shortcode in all versions up to, and including, 1.0.5. This is due to insufficient input sanitization and output escaping on the 'text' shortcode attribute. The output_shortcode() function directly concatenates the user-supplied $text variable into HTML output without applying esc_html() or any other escaping function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5711	The Post Blocks & Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sliderStyle' block attribute in the Posts Slider block in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4429	The OSM – OpenStreetMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'marker_name' and 'file_color_list' shortcode attribute of the [osm_map_v3] shortcode in all versions up to and including 6.1.15. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4025	The PrivateContent Free plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' shortcode attribute in the [pc-login-form] shortcode in all versions up to, and including, 1.2.0. This is due to insufficient input sanitization and output escaping on the 'align' attribute. Specifically, the attribute value flows from the shortcode through pc_login_form() to pc_static::form_align(), where it is directly concatenated into an HTML class attribute without esc_attr() or any 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-2026-1263	The Webling plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.9.0 due to insufficient input sanitization, insufficient output escaping, and missing capabilities checks in the 'webling_admin_save_form' and 'webling_admin_save_memberlist' functions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject Webling forms and memberlists with arbitrary web scripts that will execute whenever an administrator views the related form or memberlist area of the WordPress admin.	6.4	More Details
CVE-2026-4871	The Sports Club Management plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before' and 'after' attributes of the `scm_member_data` shortcode in all versions up to, and including, 1.12.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-57847	A container privilege escalation flaw was found in certain Ansible Automation Platform images. This issue arises from the /etc/passwd file being created with group-writable permissions during the build process. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This vulnerability allows an attacker to add a new user with any arbitrary UID, including UID 0, gaining full root privileges within the container.	6.4	More Details
CVE-2025-57175	Siklu EtherHaul 8010 siklu-uimage-nxp-enc-10_6_2-18707-ea552dc00b devices have a static root password.	6.4	More Details
CVE-	The Beaver Builder Page Builder – Drag and Drop Website Builder plugin for WordPress is vulnerable to Stored Cross-		

2026-2481	Site Scripting via the 'settings[js]' parameter in versions up to, and including, 2.10.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14732	The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widget parameters in all versions up to, and including, 3.35.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-57853	A container privilege escalation flaw was found in certain Web Terminal images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	6.4	More Details
CVE-2026-3142	The Pinterest Site Verification plugin using Meta Tag plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_var' parameter in versions up to, and including, 1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5742	The UsersWP plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 1.2.60. This is due to insufficient input sanitization of user-supplied URL fields and improper output escaping when rendering user profile data in badge widgets. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts that will execute whenever a user accesses a page containing the affected badge widget.	6.4	More Details
CVE-2026-4059	The ShopLentor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the woolentor_quickview_button shortcode's button_text attribute in all versions up to, and including, 3.3.5. This is due to insufficient input sanitization and missing output escaping on user-supplied shortcode attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2305	The AddFunc Head & Footer Code plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `aFhfc_head_code`, `aFhfc_body_code`, and `aFhfc_footer_code` post meta values in all versions up to, and including, 2.3. This is due to the plugin outputting these meta values without any sanitization or escaping. While the plugin restricts its own metabox and save handler to administrators via `current_user_can('manage_options')`, it does not use `register_meta()` with an `auth_callback` to protect these meta keys. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts via the WordPress Custom Fields interface that execute when an administrator previews or views the post.	6.4	More Details
CVE-2026-4379	The LightPress Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `group` attribute in the `[gallery]` shortcode in all versions up to, and including, 2.3.4. This is due to the plugin modifying gallery shortcode output to include the `group` attribute value without proper 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-2026-4655	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the SVG Image Widget in versions up to and including 8.4.2. This is due to insufficient input sanitization and output escaping on SVG content fetched from remote URLs in the render_svg() function. The function fetches SVG content using wp_safe_remote_get() and then directly echoes it to the page without any sanitization, only applying a preg_replace() to add attributes to the SVG tag which does not remove malicious event handlers. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary JavaScript in SVG files that will execute whenever a user accesses a page containing the malicious widget.	6.4	More Details
CVE-2026-39630	Server-Side Request Forgery (SSRF) vulnerability in Getty Images Getty Images getty-images allows Server Side Request Forgery.This issue affects Getty Images: from n/a through <= 4.1.0.	6.4	More Details
CVE-2026-6215	A weakness has been identified in DbGate up to 7.1.4. The impacted element is the function apiServerUrl1 of the file packages/rest/src/openApiDriver.ts of the component REST/GraphQL. This manipulation 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 vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-39488	Missing Authorization vulnerability in SureCart SureCart surecart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SureCart: from n/a through <= 4.0.2.	6.3	More Details
CVE-2026-6202	A security flaw has been discovered in code-projects Easy Blog Site 1.0. This affects an unknown function of the file post.php. Performing a manipulation of the argument tags results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-5302	CORS misconfiguration in CoolerControl/coolercontrold <4.0.0 allows unauthenticated remote attackers to read data and send commands to the service via malicious websites	6.3	More Details
CVE-	A security flaw has been discovered in CodeAstro Online Classroom 1.0/2.php. Affected by this vulnerability is an unknown functionality of the file /OnlineClassroom/takeassessment2.php?exid=14. Performing a manipulation of the		More

2026-6010	argument Q1 results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	6.3	Details
CVE-2026-33458	Server-Side Request Forgery (CWE-918) in Kibana One Workflow can lead to information disclosure. An authenticated user with workflow creation and execution privileges can bypass host allowlist restrictions in the Workflows Execution Engine, potentially exposing sensitive internal endpoints and data.	6.3	More Details
CVE-2026-6143	A security flaw has been discovered in farion1231 cc-switch up to 3.12.3. Affected by this issue is some unknown functionality of the file src-tauri/src/proxy/server.rs of the component ProxyServer. The manipulation results in permissive cross-domain policy with untrusted domains. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-39651	Missing Authorization vulnerability in TotalSuite Total Poll Lite totalpoll-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Total Poll Lite: from n/a through <= 4.12.0.	6.3	More Details
CVE-2026-6119	A vulnerability was identified in AstrBotDevs AstrBot up to 4.22.1. The affected element is the function post_data.get of the component API Endpoint. Such manipulation leads to server-side request forgery. The attack may be performed from remote. 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-2026-6118	A vulnerability was determined in AstrBotDevs AstrBot up to 4.22.1. Impacted is the function add_mcp_server of the file astrbot/dashboard/routes/tools.py of the component MCP Endpoint. This manipulation of the argument command causes command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-6117	A vulnerability was found in AstrBotDevs AstrBot up to 4.22.1. This issue affects the function install_plugin_upload of the file astrbot/dashboard/routes/plugin.py of the component install-upload Endpoint. The manipulation of the argument File results in sandbox issue. The attack can be executed remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-6111	A security flaw has been discovered in FoundationAgents MetaGPT up to 0.8.1. This impacts the function decode_image of the file metagpt/utils/common.py. The manipulation of the argument img_url_or_b64 results in server-side request forgery. It is possible to launch the attack 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.	6.3	More Details
CVE-2026-6125	A security flaw has been discovered in Dromara warm-flow up to 1.8.4. Impacted is the function SpelHelper.parseExpression of the file /warm-flow/save-json of the component Workflow Definition Handler. The manipulation of the argument listenerPath/skipCondition/permissionFlag results in code 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-2026-39421	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain a sandbox escape vulnerability in the ToolExecutor component. By leveraging Python's ctypes library to execute raw system calls, an authenticated attacker with workspace privileges can bypass the LD_PRELOAD-based sandbox.so module to achieve arbitrary code execution via direct kernel system calls, enabling full network exfiltration and container compromise. The library intercepts critical standard system functions such as execve, system, connect, and open. It also intercepts mprotect to prevent PROT_EXEC (executable memory) allocations within the sandboxed Python processes, but pkey_mprotect is not blocked. This issue has been fixed in version 2.8.0.	6.3	More Details
CVE-2026-39420	MaxKB is an open-source AI assistant for enterprise. In versions 2.7.1 and below, an incomplete sandbox protection mechanism allows an authenticated user with tool execution privileges to escape the LD_PRELOAD-based sandbox. By env command the attacker can clear the environment variables and drop the sandbox.so hook, leading to unrestricted Remote Code Execution (RCE) and network access. MaxKB restricts untrusted Python code execution via the Tool Debug API by injecting sandbox.so through the LD_PRELOAD environment variable. This intercepts sensitive C library functions (like execve, socket, open) to restrict network and file access. However, a patch allowed the /usr/bin/env utility to be executed by the sandboxed user. When an attacker is permitted to create subprocesses, they can execute the env -i python command. The -i flag instructs env to completely clear all environment variables before running the target program. This effectively drops the LD_PRELOAD environment variable. The newly spawned Python process will therefore execute natively without any sandbox hooks, bypassing all network and file system restrictions. This issue has been fixed in version 2.8.0.	6.3	More Details
CVE-2026-27299	Adobe Framemaker versions 2022.8 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An attacker could leverage this vulnerability to access sensitive files or data on the system. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	6.3	More Details
CVE-2026-6108	A vulnerability was found in 1Panel-dev MaxKB up to 2.6.1. The affected element is the function execute of the file apps/application/flow/step_node/mcp_node/impl/base_mcp_node.py of the component Model Context Protocol Node. Performing a manipulation results in os command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. You should 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.	6.3	More Details
CVE-2026-	Acrobat Reader versions 26.001.21411, 24.001.30360, 24.001.30362 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability that could result in arbitrary	6.3	More

34626	file system read in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		Details
CVE-2026-35165	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 21.0.0 to before 27.0.3 and 28.0.1, while the document_repository frontend was restricting file access, the backend endpoint was not correctly verifying access permissions. A user could theoretically download a file that they should not have access to, if they know or can brute force the filename. This vulnerability is fixed in 27.0.3 and 28.0.1.	6.3	More Details
CVE-2026-34985	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 16.1.0 to before 27.0.3 and 28.0.1, While the frontend of the media module filters files that the user should not have access to, the backend was not applying access checks and it would be possible for someone who should not have access to a file to access it if they know the filename. This vulnerability is fixed in 27.0.3 and 28.0.1.	6.3	More Details
CVE-2026-6191	A vulnerability was determined in itsourcecode Construction Management System 1.0. This affects an unknown function of the file /equipments.php. Executing a manipulation of the argument Name can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-6033	A vulnerability was determined in CodeAstro Online Classroom 1.0. Affected is an unknown function of the file /updatedetailsfromstudent.php?eno=146891650. Executing a manipulation of the argument fname can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-5999	A vulnerability has been found in JeecgBoot up to 3.9.1. This impacts an unknown function of the component SysAnnouncementController. Such manipulation leads to improper authorization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor confirmed the issue and will provide a fix in the upcoming release.	6.3	More Details
CVE-2026-6190	A vulnerability was found in itsourcecode Construction Management System 1.0. The impacted element is an unknown function of the file /employees.php. Performing a manipulation of the argument Name results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-6005	A flaw has been found in code-projects Patient Record Management System 1.0. The affected element is an unknown function of the file /hematology_print.php. Executing a manipulation of the argument hem_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-2026-6006	A vulnerability has been found in code-projects Patient Record Management System 1.0. The impacted element is an unknown function of the file /edit_hpatient.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-2026-6007	A vulnerability was found in itsourcecode Construction Management System 1.0. This affects an unknown function of the file /del.php. The manipulation of the argument equipname results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-5803	A security flaw has been discovered in bigsk1 openai-realtime-ui up to 188ccde27fdf3d8fab8da81f3893468f53b2797c. The affected element is an unknown function of the file server.js of the component API Proxy Endpoint. Performing a manipulation of the argument Query results in server-side request forgery. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is named 54f8f50f43af97c334a881af7b021e84b5b8310f. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-5831	A security flaw has been discovered in Agions taskflow-ai up to 2.1.8. This impacts an unknown function of the file src/mcp/server/handlers.ts of the component terminal_execute. Performing a manipulation results in os command injection. The attack is possible to be carried out remotely. Upgrading to version 2.1.9 will fix this issue. The patch is named c1550b445b9f24f38c4414e9a545f5f79f23a0fe. Upgrading the affected component is recommended. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	6.3	More Details
CVE-2026-6030	A flaw has been found in itsourcecode Construction Management System 1.0. The impacted element is an unknown function of the file /del1.php. This manipulation of the argument toolname causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2026-34861	Race condition vulnerability in the thermal management module. Impact: Successful exploitation of this vulnerability may affect availability.	6.3	More Details
CVE-2026-34862	Race condition vulnerability in the power consumption statistics module. Impact: Successful exploitation of this vulnerability may affect availability.	6.3	More Details
CVE-2026-5823	A weakness has been identified in itsourcecode Construction Management System 1.0. Affected by this issue is some unknown functionality of the file /borrowed_tool_report.php. This manipulation of the argument Home causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
	A vulnerability was determined in danielmiessler Personal_AI_Infrastructure up to 2.3.0. Affected is an unknown		

CVE-2026-6141	function of the file Skills/Parser/Tools/parse_url.ts. Executing a manipulation can lead to os command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 14322e87e58bf585cf3c7b9295578a6eb7dc4945. It is advisable to implement a patch to correct this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	6.3	More Details
CVE-2026-25204	Deserialization of untrusted data vulnerability in Samsung Open Source Escargot Java Script allows denial of service condition via process abort. This issue affects escarogt prior to commit hash 97e8115ab1110bc502b4b5e4a0c689a71520d335	6.2	More Details
CVE-2026-40227	In systemd 260 before 261, a local unprivileged user can trigger an assert via an IPC API call with an array or map that has a null element.	6.2	More Details
CVE-2026-40117	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, read_skill_file() in skill_tools.py allows reading arbitrary files from the filesystem by accepting an unrestricted skill_path parameter. Unlike file_tools.read_file which enforces workspace boundary confinement, and unlike run_skill_script which requires critical-level approval, read_skill_file has neither protection. An agent influenced by prompt injection can exfiltrate sensitive files without triggering any approval prompt. This vulnerability is fixed in 1.5.128.	6.2	More Details
CVE-2026-29628	A stack overflow in the experimental/tinyobj_loader_opt.h file of tinyobjloader commit d56555b allows attackers to cause a Denial of Service (DoS) via supplying a crafted .mtl file.	6.2	More Details
CVE-2019-25712	BlueAuditor 1.7.2.0 contains a buffer overflow vulnerability in the registration key field that allows local attackers to crash the application by submitting an oversized key value. Attackers can trigger a denial of service by entering a 256-byte buffer of repeated characters in the Key registration field, causing the application to crash during registration processing.	6.2	More Details
CVE-2026-40115	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the WSGI-based recipe registry server (server.py) reads the entire HTTP request body into memory based on the client-supplied Content-Length header with no upper bound. Combined with authentication being disabled by default (no token configured), any local process can send arbitrarily large POST requests to exhaust server memory and cause a denial of service. The Starlette-based server (serve.py) has RequestSizeLimitMiddleware with a 10MB limit, but the WSGI server lacks any equivalent protection. This vulnerability is fixed in 4.5.128.	6.2	More Details
CVE-2026-33753	rfc3161-client is a Python library implementing the Time-Stamp Protocol (TSP) described in RFC 3161. Prior to 1.0.6, an Authorization Bypass vulnerability in rfc3161-client's signature verification allows any attacker to impersonate a trusted TimeStamping Authority (TSA). By exploiting a logic flaw in how the library extracts the leaf certificate from an unordered PKCS#7 bag of certificates, an attacker can append a spoofed certificate matching the target common_name and Extended Key Usage (EKU) requirements. This tricks the library into verifying these authorization rules against the forged certificate while validating the cryptographic signature against an actual trusted TSA (such as FreeTSA), thereby bypassing the intended TSA authorization pinning entirely. This vulnerability is fixed in 1.0.6.	6.2	More Details
CVE-2026-33947	jq is a command-line JSON processor. In versions 1.8.1 and below, functions jv_setpath(), jv_getpath(), and delpaths_sorted() in jq's src/jv_aux.c use unbounded recursion whose depth is controlled by the length of a caller-supplied path array, with no depth limit enforced. An attacker can supply a JSON document containing a flat array of ~65,000 integers (~200 KB) that, when used as a path argument by a trusted jq filter, exhausts the C call stack and crashes the process with a segmentation fault (SIGSEGV). This bypass works because the existing MAX_PARSING_DEPTH (10,000) limit only protects the JSON parser, not runtime path operations where arrays can be programmatically constructed to arbitrary lengths. The impact is denial of service (unrecoverable crash) affecting any application or service that processes untrusted JSON input through jq's setpath, getpath, or delpaths builtins. This issue has been addressed in commit fb59f1491058d58bdc3e8dd28f1773d1ac690a1f.	6.2	More Details
CVE-2019-25711	SpotFTP Password Recover 2.4.2 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an oversized buffer in the Name field during registration. Attackers can generate a 256-byte payload, paste it into the Name input field, and trigger a crash when submitting the registration code.	6.2	More Details
CVE-2026-32072	Improper authentication in Windows Active Directory allows an unauthorized attacker to perform spoofing locally.	6.2	More Details
CVE-2026-40312	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below 7.1.2-19, an off by one error in the MSL decoder could result in a crash when a malicous MSL file is read. This issue has been fixed in version 7.1.2-19.	6.2	More Details
CVE-2026-40169	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below 7.1.2-19, a crafted image could result in an out of bounds heap write when writing a yaml or json output, resulting in a crash. This issue has been fixed in version 7.1.2-19.	6.2	More Details
CVE-2026-39941	ChurchCRM is an open-source church management system. Prior to 7.1.0, an XSS vulnerability allows attacker-supplied input sent via a the EName and EDesc parameters in EditEventAttendees.php to be rendered in a page without proper output encoding, enabling arbitrary JavaScript execution in victims' browsers. This vulnerability is fixed in 7.1.0.	6.1	More Details
CVE-2026-	Stack overflow vulnerability in the media platform. Impact: Successful exploitation of this vulnerability may affect availability.	6.1	More Details

34852			
CVE-2026-32088	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Biometric Service allows an unauthorized attacker to bypass a security feature with a physical attack.	6.1	More Details
CVE-2023-54364	Joomla HikaShop 4.7.4 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating GET parameters in the product filter endpoint. Attackers can craft malicious URLs containing XSS payloads in the from_option, from_ctrl, from_task, or from_itemid parameters to steal session tokens or login credentials when victims visit the link.	6.1	More Details
CVE-2025-63238	A Reflected Cross-Site Scripting (XSS) affects LimeSurvey versions prior to 6.15.11+250909, due to the lack of validation of gid parameter in getInstance() function in application/models/QuestionCreate.php. This allows an attacker to craft a malicious URL and compromise the logged in user.	6.1	More Details
CVE-2026-5226	The Optimole – Optimize Images in Real Time plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL paths in versions up to, and including, 4.2.3 This is due to insufficient output escaping on user-supplied URL paths in the get_current_url() function, which are inserted into JavaScript code via str_replace() without proper JavaScript context escaping in the replace_content() function. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-70797	Cross Site Scripting vulnerability in Limesurvey v.6.15.20+251021 allows a remote attacker to execute arbitrary code via the Box[title] and box[url] parameters.	6.1	More Details
CVE-2026-39315	Unhead is a document head and template manager. Prior to 2.1.13, useHeadSafe() is the composable that Nuxt's own documentation explicitly recommends for rendering user-supplied content in <head> safely. Internally, the hasDangerousProtocol() function in packages/unhead/src/plugins/safe.ts decodes HTML entities before checking for blocked URI schemes (javascript:, data:, vbscript:). The decoder uses two regular expressions with fixed-width digit caps. The HTML5 specification imposes no limit on leading zeros in numeric character references. When a padded entity exceeds the regex digit cap, the decoder silently skips it. The undecoded string is then passed to startsWith('javascript:'), which does not match. makeTagSafe() writes the raw value directly into SSR HTML output. The browser's HTML parser decodes the padded entity natively and constructs the blocked URI. This vulnerability is fixed in 2.1.13.	6.1	More Details
CVE-2017-20239	MDwiki contains a cross-site scripting vulnerability that allows remote attackers to execute arbitrary JavaScript by injecting malicious code through the location hash parameter. Attackers can craft URLs with JavaScript payloads in the hash fragment that are parsed and rendered without sanitization, causing the injected scripts to execute in the victim's browser context.	6.1	More Details
CVE-2026-35667	OpenClaw before 2026.3.24 contains an incomplete fix for CVE-2026-27486 where the !stop chat command uses an unpatched killProcessTree function from shell-utils.ts that sends SIGKILL immediately without graceful SIGTERM shutdown. Attackers can trigger process termination via the !stop command, causing data corruption, resource leaks, and skipped security-sensitive cleanup operations.	6.1	More Details
CVE-2026-25854	Occasional URL redirection to untrusted Site ('Open Redirect') vulnerability in Apache Tomcat via the LoadBalancerDrainingValve. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.1.0-M1 through 10.1.52, from 9.0.0.M23 through 9.0.115, from 8.5.30 through 8.5.100. Other, unsupported versions may also be affected Users are recommended to upgrade to version 11.0.20, 10.1.53 or 9.0.116, which fix the issue.	6.1	More Details
CVE-2026-32289	Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped, leading to XSS vulnerabilities.	6.1	More Details
CVE-2023-54363	Joomla Solidres 2.13.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating multiple GET parameters including show, reviews, type_id, distance, facilities, categories, prices, location, and Itemid. Attackers can craft malicious URLs containing JavaScript payloads in these parameters to steal session tokens, login credentials, or manipulate site content when victims visit the crafted links.	6.1	More Details
CVE-2025-69993	Leaflet versions up to and including 1.9.4 are vulnerable to Cross-Site Scripting (XSS) via the bindPopup() method. This method renders user-supplied input as raw HTML without sanitization, allowing attackers to inject arbitrary JavaScript code through event handler attributes (e.g., <img src=x onerror="alert('XSS')">). When a victim views an affected map popup, the malicious script executes in the context of the victim's browser session.	6.1	More Details
CVE-2023-54360	Joomla JLex Review 6.0.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the review_id URL parameter. Attackers can craft malicious links containing JavaScript payloads that execute in victims' browsers when clicked, enabling session hijacking or credential theft.	6.1	More Details
CVE-2026-5899	Insufficient policy enforcement in History Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Low)	6.1	More Details
	jq is a command-line JSON processor. In commits after 69785bf77f86e2ea1b4a20ca86775916889e91c9, the _strindices builtin in jq's src/builtin.c passes its arguments directly to jv_string_indexes() without verifying they are		

CVE-2026-39956	strings, and jv_string_indexes() in src/jv.c relies solely on assert() checks that are stripped in release builds compiled with -DNDEBUG. This allows an attacker to crash jq trivially with input like _strindices(0), and by crafting a numeric value whose IEEE-754 bit pattern maps to a chosen pointer, achieve a controlled pointer dereference and limited memory read/probe primitive. Any deployment that evaluates untrusted jq filters against a release build is vulnerable. This issue has been patched in commit fdf8ef0f0810e3d365cdd5160de43db46f57ed03.	6.1	More Details
CVE-2026-5896	Policy bypass in Audio in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass sandbox download restrictions via a crafted HTML page. (Chromium security severity: Low)	6.1	More Details
CVE-2026-31262	Cross Site Scripting vulnerability in Altenar Sportsbook Software Platform (SB2) v.2.0 allows a remote attacker to obtain sensitive information and execute arbitrary code via the URL parameter	6.1	More Details
CVE-2026-32196	Improper neutralization of input during web page generation ('cross-site scripting') in Windows Admin Center allows an unauthorized attacker to perform spoofing over a network.	6.1	More Details
CVE-2023-54362	Joomla VirtueMart Shopping-Cart 4.0.12 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the keyword parameter. Attackers can craft malicious URLs containing script payloads in the keyword parameter of the product-variants endpoint to execute arbitrary JavaScript in victim browsers and steal session tokens or credentials.	6.1	More Details
CVE-2026-21904	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the list filter field that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R5 Patch V3.	6.1	More Details
CVE-2026-6203	The User Registration & Membership plugin for WordPress is vulnerable to Open Redirect in versions up to and including 5.1.4. This is due to insufficient validation of user-supplied URLs passed via the 'redirect_to_on_logout' GET parameter before redirecting users. The `redirect_to_on_logout` GET parameter is passed directly to WordPress's `wp_redirect()` function instead of the domain-restricted `wp_safe_redirect()`. While `esc_url_raw()` is applied to sanitize malformed URLs, it does not restrict the redirect destination to the local domain, allowing an attacker to craft a specially formed link that redirects users to potentially malicious external URLs after logout, which could be used to facilitate phishing attacks.	6.1	More Details
CVE-2026-26169	Buffer over-read in Windows Kernel Memory allows an authorized attacker to disclose information locally.	6.1	More Details
CVE-2026-0512	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP Supplier Relationship Management (SICF Handler in SRM Catalog), an unauthenticated attacker could craft a malicious URL, that if accessed by a victim, results in execution of malicious content within the victim's browser. This could allow the attacker to access and modify information, impacting the confidentiality and integrity of the application, while availability remains unaffected.	6.1	More Details
CVE-2023-54361	Joomla iProperty Real Estate 4.1.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the filter_keyword parameter. Attackers can craft URLs containing JavaScript payloads in the filter_keyword GET parameter of the all-properties-with-map endpoint to execute arbitrary code in victim browsers and steal session tokens or credentials.	6.1	More Details
CVE-2026-4305	The Royal WordPress Backup & Restore Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wpr_pending_template' parameter in all versions up to, and including, 1.0.16 due to insufficient input validation. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-27674	Due to a Code Injection vulnerability in SAP NetWeaver Application Server Java (Web Dynpro Java), an unauthenticated attacker could supply crafted input that is interpreted by the application and causes it to reference attacker-controlled content. If a victim accesses the affected functionality, that attacker-controlled content could be executed in the victim&#65533;s browser, potentially resulting in session compromise. This could allow the attacker to execute arbitrary client-side code, impacting the confidentiality and integrity of the application, with no impact to availability.	6.1	More Details
CVE-2026-34257	Due to an Open Redirect vulnerability in SAP NetWeaver Application Server ABAP, an unauthenticated attacker could craft malicious URL that, if accessed by a victim, they could be redirected to the page controlled by the attacker. This causes low impact on confidentiality and integrity of the application with no impact on availability.	6.1	More Details
CVE-2026-34614	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed.	6.1	More Details
CVE-2023-54358	WordPress adivaha Travel Plugin 2.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the isMobile parameter. Attackers can craft malicious URLs containing JavaScript payloads in the isMobile GET parameter at the /mobile-app/v3/ endpoint to execute arbitrary code in victims' browsers and steal session tokens or credentials.	6.1	More Details
CVE-2025-	A cross-site scripting (XSS) vulnerability in rrweb-snapshot before v2.0.0-alpha.18 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details

45806			
CVE-2026-21331	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed.	6.1	More Details
CVE-2026-4394	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Credit Card field's 'Card Type' sub-field (`input_<id>.4`) in all versions up to, and including, 2.9.30. This is due to the `get_value_entry_detail()` method in the `GF_Field_CreditCard` class outputting the card type value without escaping, combined with `get_value_save_entry()` accepting and storing unsanitized user input for the `input_<id>.4` parameter. The Card Type field is not rendered on the frontend form (it is normally derived from the card number), but the backend submission parser blindly accepts it if included in the POST request. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the form entry in the WordPress dashboard.	6.1	More Details
CVE-2025-65136	In manikandan580 School-management-system 1.0, a reflected XSS vulnerability exists in /studentms/admin/contact-us.php via the pagedes POST parameter.	6.1	More Details
CVE-2025-65132	alandsilva26 hotel-management-php 1.0 is vulnerable to Cross Site Scripting (XSS) in /public/admin/edit_room.php which allows an attacker to inject and execute arbitrary JavaScript via the room_id GET parameter.	6.1	More Details
CVE-2026-33822	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	6.1	More Details
CVE-2025-68649	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.7, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.7, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.7, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow a privileged attacker to delete files from the underlying filesystem via crafted CLI requests.	6.0	More Details
CVE-2026-39670	Server-Side Request Forgery (SSRF) vulnerability in Brecht Visual Link Preview visual-link-preview allows Server Side Request Forgery.This issue affects Visual Link Preview: from n/a through <= 2.3.0.	6.0	More Details
CVE-2026-5525	A stack-based buffer overflow vulnerability exists in Notepad++ version 8.9.3 in the file drop handler component. When a user drags and drops a directory path of exactly 259 characters without a trailing backslash, the application appends a backslash and null terminator without proper bounds checking, resulting in a stack buffer overflow and application crash (STATUS_STACK_BUFFER_OVERRUN).	6.0	More Details
CVE-2026-39810	A use of hard-coded cryptographic key vulnerability in Fortinet FortiClientEMS 7.4.0 through 7.4.5 may allow attacker to information disclosure via decrypting database dump.	6.0	More Details
CVE-2025-61624	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [CWE-22] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.7.0, 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 7.6.4, FortiProxy 7.4.0 through 7.4.11, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions, FortiSwitchManager 7.2.0 through 7.2.7, FortiSwitchManager 7.0.0 through 7.0.6 may allow an authenticated attacker with admin profile and at least read-write permissions to write or delete arbitrary files via specific CLI commands.	6.0	More Details
CVE-2026-39683	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chief Gnome Garden Gnome Package garden-gnome-package allows DOM-Based XSS.This issue affects Garden Gnome Package: from n/a through <= 2.4.1.	5.9	More Details
CVE-2026-39865	Axios is a promise based HTTP client for the browser and Node.js. Starting in version 1.13.0 and prior to 1.13.2, Axios HTTP/2 session cleanup logic contains a state corruption bug that allows a malicious server to crash the client process through concurrent session closures. The vulnerability exists in the Http2Sessions.getSession() method in lib/adapters/http.js. The session cleanup logic contains a control flow error when removing sessions from the sessions array. This vulnerability is fixed in 1.13.2.	5.9	More Details
CVE-2026-39667	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jongmyoung Kim Korea SNS korea-sns allows DOM-Based XSS.This issue affects Korea SNS: from n/a through <= 1.7.0.	5.9	More Details
CVE-2026-35622	OpenClaw before 2026.3.22 contains an improper authentication verification vulnerability in Google Chat app-url webhook handling that accepts add-on principals outside intended deployment bindings. Attackers can bypass webhook authentication by providing non-deployment add-on principals to execute unauthorized actions through the Google Chat integration.	5.9	More Details
CVE-2026-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zookatron MyBookTable Bookstore mybooktable allows Stored XSS.This issue affects MyBookTable Bookstore: from n/a through	5.9	More Details

39604	<= 3.6.0.		
CVE-2026-32226	Concurrent execution using shared resource with improper synchronization ('race condition') in .NET Framework allows an unauthorized attacker to deny service over a network.	5.9	More Details
CVE-2026-39638	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Qubely qubely allows Stored XSS.This issue affects Qubely: from n/a through <= 1.8.14.	5.9	More Details
CVE-2026-39541	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Hydra Booking hydra-booking allows Stored XSS.This issue affects Hydra Booking: from n/a through <= 1.1.38.	5.9	More Details
CVE-2026-39844	NiceGUI is a Python-based UI framework. Prior to 3.10.0, Since PurePosixPath only recognizes forward slashes (/) as path separators, an attacker can bypass this sanitization on Windows by using backslashes (\) in the upload filename. Applications that construct file paths using file.name (a pattern demonstrated in NiceGUI's bundled examples) are vulnerable to arbitrary file write on Windows. This vulnerability is fixed in 3.10.0.	5.9	More Details
CVE-2026-34859	UAF vulnerability in the kernel module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	5.9	More Details
CVE-2026-39693	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fesomia FSM Custom Featured Image Caption fsm-custom-featured-image-caption allows DOM-Based XSS.This issue affects FSM Custom Featured Image Caption: from n/a through <= 1.25.1.	5.9	More Details
CVE-2026-39615	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shahjada Download Manager download-manager allows Stored XSS.This issue affects Download Manager: from n/a through <= 3.3.53.	5.9	More Details
CVE-2026-33900	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below both 7.1.2-19 and 6.9.13-44, the viff encoder contains an integer truncation/wraparound issue on 32-bit builds that could trigger an out of bounds heap write, potentially causing a crash. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.9	More Details
CVE-2026-35670	OpenClaw before 2026.3.22 contains a webhook reply delivery vulnerability that allows attackers to rebind chat replies to unintended users by exploiting mutable username matching instead of stable numeric user identifiers. Attackers can manipulate username changes to redirect webhook-triggered replies to different users, bypassing the intended recipient binding recorded in webhook events.	5.9	More Details
CVE-2026-5300	Unauthenticated functionality in CoolerControl/coolercontrold <4.0.0 allows unauthenticated attackers to view and modify potentially sensitive data via HTTP requests	5.9	More Details
CVE-2026-35597	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the TOTP failed-attempt lockout mechanism is non-functional due to a database transaction handling bug. When a TOTP validation fails, the login handler in pkg/routes/api/v1/login.go calls HandleFailedTOTPAuth and then unconditionally rolls back. HandleFailedTOTPAuth in pkg/user/totp.go uses an in-memory counter (key-value store) to track failed attempts. When the counter reaches 10, it calls user.SetStatus(s, StatusAccountLocked) on the same database session s. Because the login handler always rolls back after a TOTP failure, the StatusAccountLocked write is undone. The in-memory counter correctly increments past 10, so the lockout code executes on every subsequent attempt, but the database write is rolled back every time. This allows unlimited brute-force attempts against TOTP codes. This vulnerability is fixed in 2.3.0.	5.9	More Details
CVE-2026-33773	An Incorrect Initialization of Resource vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX Series and QFX Series device allows an unauthenticated, network-based attacker to cause an integrity impact to downstream networks. When the same family inet or inet6 filter is applied on an IRB interface and on a physical interface as egress filter on EX4100, EX4400, EX4650 and QFX5120 devices, only one of the two filters will be applied, which can lead to traffic being sent out one of these interfaces which should have been blocked. This issue affects Junos OS on EX Series and QFX Series: * 23.4 version 23.4R2-S6, * 24.2 version 24.2R2-S3. No other Junos OS versions are affected.	5.8	More Details
CVE-2026-1516	GitLab has remediated an issue in GitLab EE affecting all versions from 18.0.0 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that in Code Quality reports could have allowed an authenticated user to leak IP addresses of users viewing the report via specially crafted content.	5.7	More Details
CVE-2026-30816	An external control of configuration vulnerability in the OpenVPN module of TP-Link AX53 v1.0 allows an authenticated adjacent attacker to read arbitrary file when a malicious configuration file is processed. Successful exploitation may allow unauthorized access to arbitrary files on the device, potentially exposing sensitive information.This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	5.7	More Details
CVE-2026-34855	Out-of-bounds write vulnerability in the kernel module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	5.7	More Details
CVE-	UAF vulnerability in the kernel module. Impact: Successful exploitation of this vulnerability will affect availability and		More

2026-34854	confidentiality.	5.7	Details
CVE-2026-39901	monetr is a budgeting application focused on planning for recurring expenses. Prior to 1.12.3, a transaction integrity flaw allows an authenticated tenant user to soft-delete synced non-manual transactions through the transaction update endpoint, despite the application explicitly blocking deletion of those transactions via the normal DELETE path. This bypass undermines the intended protection for imported transaction records and allows protected transactions to be hidden from normal views. This vulnerability is fixed in 1.12.3.	5.7	More Details
CVE-2026-21742	A cleartext transmission of sensitive information vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated attacker to view cleartext password in response for Secure Message Exchange and Radius queries, if configured	5.7	More Details
CVE-2026-30817	An external configuration control vulnerability in the OpenVPN module of TP-Link AX53 v1.0 allows an authenticated adjacent attacker to read arbitrary files when a malicious configuration file is processed. Successful exploitation may allow unauthorized access to arbitrary files on the device, potentially exposing sensitive information.This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	5.7	More Details
CVE-2026-35655	OpenClaw before 2026.3.22 contains an identity spoofing vulnerability in ACP permission resolution that trusts conflicting tool identity hints from rawInput and metadata. Attackers can spoof tool identities through rawInput parameters to suppress dangerous-tool prompting and bypass security restrictions.	5.7	More Details
CVE-2026-23653	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio Code allows an authorized attacker to disclose information over a network.	5.7	More Details
CVE-2026-4913	Improper protection of an alternate path in Ivanti N-ITSM before version 2025.4 allows a remote authenticated attacker to retain access when their account has been disabled.	5.7	More Details
CVE-2026-23670	Untrusted pointer dereference in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to bypass a security feature locally.	5.7	More Details
CVE-2026-40190	LangSmith Client SDKs provide SDK's for interacting with the LangSmith platform. Prior to 0.5.18, the LangSmith JavaScript/TypeScript SDK (langsmith) contains an incomplete prototype pollution fix in its internally vendored lodash set() utility. The baseAssignValue() function only guards against the __proto__ key, but fails to prevent traversal via constructor.prototype. This allows an attacker who controls keys in data processed by the createAnonymizer() API to pollute Object.prototype, affecting all objects in the Node.js process. This vulnerability is fixed in 0.5.18.	5.6	More Details
CVE-2026-6011	A weakness has been identified in OpenClaw up to 2026.1.26. Affected by this issue is some unknown functionality of the file src/agents/tools/web-fetch.ts of the component assertPublicHostname Handler. Executing a manipulation can lead to server-side request forgery. The attack can be executed remotely. This attack is characterized by high complexity. The exploitation is known to be difficult. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2026.1.29 can resolve this issue. This patch is called b623557a2ec7e271bda003eb3ac33fbb2e218505. Upgrading the affected component is advised.	5.6	More Details
CVE-2026-34867	Double free vulnerability in the multi-mode input system. Impact: Successful exploitation of this vulnerability may affect availability.	5.6	More Details
CVE-2026-27222	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Divide By Zero vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application or render it unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-39390	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.4.0, the Google Maps iframe setting (cMap field) in compInfosPost() sanitizes input using strip_tags() with an <iframe> allowlist and regex-based removal of on\w+ event handlers. However, the srcdoc attribute is not an event handler and passes all filters. An attacker with admin settings access can inject an <iframe srcdoc="..."> payload with HTML-entity-encoded JavaScript that executes in the context of the parent page when rendered to unauthenticated frontend visitors. This vulnerability is fixed in 0.31.4.0.	5.5	More Details
CVE-2026-32081	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-32079	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-32288	tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive containing a large number of sparse regions encoded in the "old GNU sparse map" format.	5.5	More Details
CVE-	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information		More

2026-32218	locally.	5.5	Details
CVE-2026-27285	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application or disrupt its functionality. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-27930	Out-of-bounds read in Windows GDI allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2026-33902	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below both 7.1.2-19 and 6.9.13-44, a stack overflow vulnerability in ImageMagick's FX expression parser allows an attacker to crash the process by providing a deeply nested expression. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.5	More Details
CVE-2026-27931	Out-of-bounds read in Windows GDI allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2026-39464	Server-Side Request Forgery (SSRF) vulnerability in SeedProd Coming Soon Page, Under Construction & Maintenance Mode by SeedProd coming-soon allows Server Side Request Forgery.This issue affects Coming Soon Page, Under Construction & Maintenance Mode by SeedProd: from n/a through <= 6.19.8.	5.5	More Details
CVE-2026-27300	Adobe Framemaker versions 2022.8 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-32181	Improper privilege management in Microsoft Windows allows an authorized attacker to deny service locally.	5.5	More Details
CVE-2026-39392	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.4.0, the Pages module does not apply the html_purify validation rule to content fields during create and update operations, while the Blog module does. Page content is stored unsanitized in the database and rendered as raw HTML on the public frontend via echo $pageInfo->content. An authenticated admin with page-editing privileges can inject arbitrary JavaScript that executes in the browser of every public visitor viewing the page. This vulnerability is fixed in 0.31.4.0.	5.5	More Details
CVE-2026-39855	osslsigncode is a tool that implements Authenticode signing and timestamping. Prior to 2.13, an integer underflow vulnerability exists in osslsigncode version 2.12 and earlier in the PE page-hash computation code (pe_page_hash_calc()). When page hash processing is performed on a PE file, the function subtracts hdrsize from pagesize without first validating that pagesize >= hdrsize. If a malicious PE file sets SizeOfHeaders (hdrsize) larger than SectionAlignment (pagesize), the subtraction underflows and produces a very large unsigned length. The code allocates a zero-filled buffer of pagesize bytes and then attempts to hash pagesize - hdrsize bytes from that buffer. After the underflow, this results in an out-of-bounds read from the heap and can crash the process. The vulnerability can be triggered while signing a malicious PE file with page hashing enabled (-ph), or while verifying a malicious signed PE file that already contains page hashes. Verification of an already signed file does not require the verifier to pass -ph. This vulnerability is fixed in 2.13.	5.5	More Details
CVE-2026-20806	Access of resource using incompatible type ('type confusion') in Windows COM allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-33103	Improper access control in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-39856	osslsigncode is a tool that implements Authenticode signing and timestamping. Prior to 2.13, an out-of-bounds read vulnerability exists in osslsigncode version 2.12 and earlier in the PE page-hash computation code (pe_page_hash_calc()). When processing PE sections for page hashing, the function uses PointerToRawData and SizeOfRawData values from section headers without validating that the referenced region lies within the mapped file. An attacker can craft a PE file with section headers that point beyond the end of the file. When osslsigncode computes page hashes for such a file, it may attempt to hash data from an invalid memory region, causing an out-of-bounds read and potentially crashing the process. The vulnerability can be triggered while signing a malicious PE file with page hashing enabled (-ph), or while verifying a malicious signed PE file that already contains page hashes. Verification of an already signed file does not require the verifier to pass -ph. This vulnerability is fixed in 2.13.	5.5	More Details
CVE-2026-33905	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below both 7.1.2-19 and 6.9.13-44, the -sample operation has an out of bounds read when an specific offset is set through the `sample:offset` define that could lead to an out of bounds read. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.5	More Details
CVE-2026-32217	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details

CVE-2026-33787	An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis control daemon (chassisd) of Juniper Networks Junos OS on SRX1500, SRX4100, SRX4200 and SRX4600 allows a local attacker with low privileges to cause a complete Denial of Service (DoS). When a specific 'show chassis' CLI command is executed, chassisd crashes and restarts which causes a momentary impact to all traffic until all modules are online again. This issue affects Junos OS on SRX1500, SRX4100, SRX4200 and SRX4600: * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7 * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R1-S1, 25.2R2.	5.5	More Details
CVE-2026-40183	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below 7.1.2-19, the JXL encoder has an heap write overflow when a user specifies that the image should be encoded as 16 bit floats. This issue has been fixed in version 7.1.2-19.	5.5	More Details
CVE-2026-40310	ImageMagick is free and open-source software used for editing and manipulating digital images. Versions below both 7.1.2-19 and 6.9.13-44, contain a heap out-of-bounds write in the JP2 encoder with when a user specifies an invalid sampling index. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.5	More Details
CVE-2026-40311	ImageMagick is free and open-source software used for editing and manipulating digital images. Versions below 7.1.2-19 and 6.9.13-44 contain a heap use-after-free vulnerability that can cause a crash when reading and printing values from an invalid XMP profile. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.5	More Details
CVE-2026-35477	InvenTree is an Open Source Inventory Management System. From 1.2.3 to 1.2.6, the fix for CVE-2026-27629 upgraded the PART_NAME_FORMAT validator to use jinja2.sandbox.SandboxedEnvironment. However, the actual renderer in part/helpers.py was not updated and still uses the non-sandboxed jinja2.Environment. Additionally, the validator uses a dummy Part instance with pk=None, which allows conditional template expressions to behave differently during validation versus production rendering. A staff user with settings access can craft a template that passes validation but executes arbitrary code during rendering. This issue requires access by a user with granted staff permissions. This vulnerability is fixed in 1.2.7 and 1.3.0.	5.5	More Details
CVE-2026-32212	Improper link resolution before file access ('link following') in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-32214	Improper access control in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-32215	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-32216	Null pointer dereference in Windows Redirected Drive Buffering allows an authorized attacker to deny service locally.	5.5	More Details
CVE-2026-33776	A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS and Junos OS Evolved allows a local user with low privileges to read sensitive information. A local user with low privileges can execute the CLI command 'show mgd' with specific arguments which will expose sensitive information. This issue affects Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S1, * 25.2 version before 25.2R1-S2, 25.2R2; Junos OS Evolved: * all versions before 23.2R2-S6-EVO, * 23.4 version before 23.4R2-S6-EVO, * 24.2 version before 24.2R2-S4-EVO, * 24.4 versions before 24.4R2-S1-EVO, * 25.2 versions before 25.2R2-EVO.	5.5	More Details
CVE-2026-27258	DNG SDK versions 1.7.1 2502 and earlier are affected by an out-of-bounds write vulnerability that could lead to application denial-of-service. An attacker could leverage this vulnerability to corrupt memory, causing the application to crash or become unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-40159	PraisonAI is a multi-agent teams system. Prior to 4.5.128, PraisonAI's MCP (Model Context Protocol) integration allows spawning background servers via stdio using user-supplied command strings (e.g., MCP("npx -y @smithery/cli ...")). These commands are executed through Python's subprocess module. By default, the implementation forwards the entire parent process environment to the spawned subprocess. As a result, any MCP command executed in this manner inherits all environment variables from the host process, including sensitive data such as API keys, authentication tokens, and database credentials. This behavior introduces a security risk when untrusted or third-party commands are used. In common scenarios where MCP tools are invoked via package runners such as npx -y, arbitrary code from external or potentially compromised packages may execute with access to these inherited environment variables. This creates a risk of unintended credential exposure and enables potential supply chain attacks through silent exfiltration of secrets. This vulnerability is fixed in 4.5.128.	5.5	More Details
CVE-2026-33786	An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis control daemon (chassisd) of Juniper Networks Junos OS on SRX1600, SRX2300 and SRX4300 allows a local attacker with low privileges to cause a complete Denial of Service (DoS). When a specific 'show chassis' CLI command is executed, chassisd crashes and restarts which causes a momentary impact to all traffic until all modules are online again. This issue affects Junos OS on SRX1600, SRX2300 and SRX4300: * 24.4 versions before 24.4R1-S3, 24.4R2. This issue does not affect Junos OS versions before 24.4R1.	5.5	More Details
CVE-	HDF5 is software for managing data. In 1.14.1-2 and earlier, an attacker who can control an h5 file parsed by HDF5		

2026-29043	can trigger a write-based heap buffer overflow condition in the H5T__ref_mem_setnull method. This can lead to a denial-of-service condition, and potentially further issues such as remote code execution depending on the practical exploitability of the heap overflow against modern operating systems.	5.5	More Details
CVE-2026-32084	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-27301	Adobe Framemaker versions 2022.8 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-27286	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-32085	Exposure of sensitive information to an unauthorized actor in Windows Remote Procedure Call allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-40112	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the Flask API endpoint in src/praisonai/api.py renders agent output as HTML without effective sanitization. The _sanitize_html function relies on the nh3 library, which is not listed as a required or optional dependency in pyproject.toml. When nh3 is absent (the default installation), the sanitizer is a no-op that returns HTML unchanged. An attacker who can influence agent input (via RAG data poisoning, web scraping results, or prompt injection) can inject arbitrary JavaScript that executes in the browser of anyone viewing the API output. This vulnerability is fixed in 4.5.128.	5.4	More Details
CVE-2024-23104	An exposure of sensitive information to an unauthorized actor vulnerability in Fortinet FortiNDR 7.6.0, FortiNDR 7.4.0 through 7.4.8, FortiNDR 7.2 all versions, FortiNDR 7.1 all versions, FortiNDR 7.0 all versions, FortiVoice 7.0.0 through 7.0.1 may allow a remote authenticated attacker with at least read-only permission on system maintenance to access backup information via crafted HTTP requests	5.4	More Details
CVE-2026-4914	Stored XSS in Ivanti N-ITSM before version 2025.4 allows a remote authenticated attacker to obtain limited information from other user sessions. User interaction is required.	5.4	More Details
CVE-2026-5811	A vulnerability was identified in SourceCodester Online Food Ordering System 1.0. Affected by this issue is the function save_product of the file /Actions.php of the component POST Parameter Handler. Such manipulation of the argument price leads to business logic errors. The attack may be performed from remote. The exploit is publicly available and might be used.	5.4	More Details
CVE-2026-39603	Cross-Site Request Forgery (CSRF) vulnerability in ThemeGoods Grand Photography grandphotography allows Cross Site Request Forgery.This issue affects Grand Photography: from n/a through <= 5.7.8.	5.4	More Details
CVE-2026-4401	The Download Monitor plugin for WordPress is vulnerable to Cross-Site Request Forgery in the `actions_handler()` and `bulk_actions_handler()` methods in `class-dlm-downloads-path.php` in all versions up to, and including, 5.1.10. This is due to missing nonce verification on these functions. This makes it possible for unauthenticated attackers to delete, disable, or enable approved download paths via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2026-3781	The Attendance Manager plugin for WordPress is vulnerable to SQL Injection via the 'attmgr_off' parameter in all versions up to, and including, 0.6.2. This is 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.	5.4	More Details
CVE-2026-0811	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.9. This is due to missing or incorrect nonce validation on the 'vsz_cf7_save_setting_callback' function. This makes it possible for unauthenticated attackers to delete form entry via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2026-39635	Cross-Site Request Forgery (CSRF) vulnerability in ThemeGoods Grand Magazine grandmagazine allows Cross Site Request Forgery.This issue affects Grand Magazine: from n/a through <= 3.5.5.	5.4	More Details
CVE-2026-4124	The Ziggeo plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.1.1. The wp_ajax_ziggeo_ajax handler only verifies a nonce (check_ajax_referer) but performs no capability checks via current_user_can(). Furthermore, the nonce ('ziggeo_ajax_nonce') is exposed to all logged-in users on every page via the wp_head and admin_head hooks . This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke multiple administrative operations including: saving arbitrary translation strings (translations_panel_save_strings via update_option('ziggeo_translations')), creating/updating/deleting event templates (event_editor_save_template/update_template/remove_template via update_option('ziggeo_events')), modifying SDK application settings (sdk_applications operations), and managing notifications (notification_handler via update_option('ziggeo_notifications')).	5.4	More Details
	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, task titles are embedded directly into		

CVE-2026-35600	Markdown link syntax in overdue email notifications without escaping Markdown special characters. When rendered by goldmark and sanitized by bluemonday (which allows <a> and <img> tags), injected Markdown constructs produce phishing links and tracking pixels in legitimate notification emails. This vulnerability is fixed in 2.3.0.	5.4	More Details
CVE-2025-1794	The AM LottiePlayer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via uploaded SVG files in all versions up to, and including, 3.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2026-39634	Cross-Site Request Forgery (CSRF) vulnerability in ThemeGoods Grand Portfolio grandportfolio allows Cross Site Request Forgery.This issue affects Grand Portfolio: from n/a through <= 3.3.	5.4	More Details
CVE-2026-39614	Missing Authorization vulnerability in ilGhera JW Player for WordPress jw-player-7-for-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JW Player for WordPress: from n/a through <= 2.3.6.	5.4	More Details
CVE-2026-39607	Missing Authorization vulnerability in Wpbens Filter Plus filter-plus allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Filter Plus: from n/a through <= 1.1.17.	5.4	More Details
CVE-2026-5812	A security flaw has been discovered in SourceCodester Pharmacy Product Management System 1.0. This affects an unknown part of the file add-sales.php of the component POST Parameter Handler. Performing a manipulation of the argument txtqty results in business logic errors. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	5.4	More Details
CVE-2026-6201	A vulnerability was identified in CodeAstro Online Job Portal 1.0. The impacted element is an unknown function of the file /jobs/job-delete.php of the component Delete Job Posting Handler. Such manipulation of the argument ID leads to improper access controls. The attack can be launched remotely. The exploit is publicly available and might be used.	5.4	More Details
CVE-2026-33740	EspoCRM is an open source customer relationship management application. In versions 9.3.3 and below, the POST /api/v1/Email/importEml endpoint contains an Insecure Direct Object Reference (IDOR) vulnerability where the attacker-supplied fileId parameter is used to fetch any attachment directly from the repository without verifying that the current user has authorization to access it. Any authenticated user with Email:create and Import permissions can exploit this to read another user's .eml attachment contents by importing them as a new email into the attacker's mailbox, while the original victim attachment record is deleted as a side effect of the import flow. This is inconsistent with the standard attachment download path, which enforces ACL checks before returning file data, and is practically exploitable because attachment IDs are commonly exposed in normal UI and API workflows such as stream payloads and download links. This issue is fixed in version 9.3.4.	5.4	More Details
CVE-2026-4332	GitLab has remediated an issue in GitLab EE affecting all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that, in customizable analytics dashboards, could have allowed an authenticated user to execute arbitrary JavaScript in the context of other users' browsers due to improper input sanitization.	5.4	More Details
CVE-2026-35602	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the Vikunja file import endpoint uses the attacker-controlled Size field from the JSON metadata inside the import zip instead of the actual decompressed file content length for the file size enforcement check. By setting Size to 0 in the JSON while including large compressed file entries in the zip, an attacker bypasses the configured maximum file size limit. This vulnerability is fixed in 2.3.0.	5.4	More Details
CVE-2026-35565	Stored Cross-Site Scripting (XSS) via Unsanitized Topology Metadata in Apache Storm UI Versions Affected: before 2.8.6 Description: The Storm UI visualization component interpolates topology metadata including component IDs, stream names, and grouping values directly into HTML via innerHTML in parseNode() and parseEdge() without sanitization at any layer. An authenticated user with topology submission rights could craft a topology containing malicious HTML/JavaScript in component identifiers (e.g., a bolt ID containing an onerror event handler). This payload flows through Nimbus → Thrift → the Visualization API → vis.js tooltip rendering, resulting in stored cross-site scripting. In multi-tenant deployments where topology submission is available to less-trusted users but the UI is accessed by operators or administrators, this enables privilege escalation through script execution in an admin's browser session. Mitigation: 2.x users should upgrade to 2.8.6. Users who cannot upgrade immediately should monkey-patch the parseNode() and parseEdge() functions in the visualization JavaScript file to HTML-escape all API-supplied values including nodeId, :capacity, :latency, :component, :stream, and :grouping before interpolation into tooltip HTML strings, and should additionally restrict topology submission to trusted users via Nimbus ACLs as a defense-in-depth measure. A guide on how to do this is available in the release notes of 2.8.6. Credit: This issue was discovered while investigating another report by K.	5.4	More Details
CVE-2026-32893	Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, a Reflected Cross-Site Scripting (XSS) vulnerability in the exercise question list admin panel allows an attacker to execute arbitrary JavaScript in an authenticated teacher's browser. The pagination code merges all $_GET parameters via array_merge() and outputs the result via http_build_query() directly into HTML href attributes without htmlspecialchars() encoding. This vulnerability is fixed in 2.0.0-RC.3.	5.4	More Details
CVE-2026-34623	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a specially crafted web page.	5.4	More Details

CVE-2026-39647	Server-Side Request Forgery (SSRF) vulnerability in sonaar MP3 Audio Player for Music, Radio & Podcast by Sonaar mp3-music-player-by-sonaar allows Server Side Request Forgery.This issue affects MP3 Audio Player for Music, Radio & Podcast by Sonaar: from n/a through <= 5.11.	5.4	More Details
CVE-2026-40071	pyLoad is a free and open-source download manager written in Python. Prior to 0.5.0b3.dev97, the /json/package_order, /json/link_order, and /json/abort_link WebUI JSON endpoints enforce weaker permissions than the core API methods they invoke. This allows authenticated low-privileged users to execute MODIFY operations that should be denied by pyLoad's own permission model. This vulnerability is fixed in 0.5.0b3.dev97.	5.4	More Details
CVE-2026-39504	Missing Authorization vulnerability in InstaWP InstaWP Connect instawp-connect allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects InstaWP Connect: from n/a through <= 0.1.2.5.	5.4	More Details
CVE-2025-61886	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.4, FortiSandbox PaaS 5.0.0 through 5.0.4 may allow an attacker to perform an XSS attack via crafted HTTP requests.	5.4	More Details
CVE-2026-24069	Kiuwan SAST improperly authorizes SSO logins for locally disabled mapped user accounts, allowing disabled users to continue accessing the application. Kiuwan Cloud was affected, and Kiuwan SAST on-premise (KOP) was affected before 2.8.2509.4.	5.4	More Details
CVE-2026-34624	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage.	5.4	More Details
CVE-2026-39645	Server-Side Request Forgery (SSRF) vulnerability in Global Payments GlobalPayments WooCommerce global-payments-woocommerce allows Server Side Request Forgery.This issue affects GlobalPayments WooCommerce: from n/a through <= 1.18.0.	5.4	More Details
CVE-2026-34212	Docmost is open-source collaborative wiki and documentation software. In versions prior to 0.71.0, improper neutralization of attachment URLs in Docmost allows a low-privileged authenticated user to store a malicious `javascript:` URL inside an attachment node in page content. When another user views the page and activates the attachment link/icon, attacker-controlled JavaScript executes in the context of the Docmost origin. Version 0.71.0 patches the issue.	5.4	More Details
CVE-2026-39526	Authorization Bypass Through User-Controlled Key vulnerability in wpstream WpStream wpstream allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WpStream: from n/a through < 4.11.2.	5.4	More Details
CVE-2026-34213	Docmost is open-source collaborative wiki and documentation software. Starting in version 0.3.0 and prior to version 0.71.0, improper authorization in Docmost allows a low-privileged authenticated user to overwrite another page's attachment within the same workspace by supplying a victim `attachmentId` to `POST /api/files/upload`. This is a remote integrity issue requiring no victim interaction. Version 0.71.0 contains a patch.	5.4	More Details
CVE-2026-35620	OpenClaw before 2026.3.24 contains missing authorization vulnerabilities in the /send and /allowlist chat command handlers. The /send command allows non-owner command-authorized senders to change owner-only session delivery policy settings, and the /allowlist mutating commands fail to enforce operator.admin scope. Attackers with operator.write scope can invoke /send on|off|inherit to persistently mutate the current session's sendPolicy, and execute /allowlist add commands to modify config-backed allowFrom entries and pairing-store allowlist entries without proper admin authorization.	5.4	More Details
CVE-2026-5895	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 147.0.7727.55 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. (Chromium security severity: Low)	5.4	More Details
CVE-2026-3358	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized private course enrollment in all versions up to, and including, 3.9.7. This is due to missing post_status validation in the `enroll_now()` and `course_enrollment()` functions. Both enrollment endpoints verify the nonce, user authentication, and whether the course is purchasable, but fail to check if the course has a `private` post_status. This makes it possible for authenticated attackers with Subscriber-level access or above to enroll in private courses by sending a crafted POST request with the target course ID. The enrollment record is created in the database and the private course title and enrollment status are exposed in the subscriber's dashboard, though WordPress core access control prevents the subscriber from viewing the actual course content (returns 404). Enrollment in private courses should be restricted to users with the `read_private_posts` capability.	5.4	More Details
CVE-2026-27288	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage.	5.4	More Details
CVE-2026-34625	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage.	5.4	More Details
CVE-	OpenStack Skyline before 5.0.1, 6.0.0, and 7.0.0 has a DOM-based Cross-Site Scripting (XSS) vulnerability in the		

2026-40212	console because document.write is used unsafely, which is relevant in scenarios where administrators use the console web interface to view instance console logs.	5.4	More Details
CVE-2026-39695	Server-Side Request Forgery (SSRF) vulnerability in podigee Podigee podigee allows Server Side Request Forgery.This issue affects Podigee: from n/a through <= 1.4.0.	5.4	More Details
CVE-2026-33119	User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2025-63743	Cross-Site Scripting vulnerability in the Snipe-IT web-based asset management system v8.3.0 to up and including v8.3.1 allows authenticated attacker with lowest privileges sufficient only to log in, to inject arbitrary JavaScript code via "Name" and "Surname" fields. The JavaScript code is executed whenever "Activity Report" or modified profile is viewed directly by any user with sufficient permissions. Successful exploitation of this issue requires that the profile's "Display Name" is not set. The vulnerability is fixed in v8.3.2.	5.4	More Details
CVE-2026-39710	Cross-Site Request Forgery (CSRF) vulnerability in stmcan RT-Theme 18 | Extensions rt18-extensions allows Cross Site Request Forgery.This issue affects RT-Theme 18 | Extensions: from n/a through <= 2.5.	5.4	More Details
CVE-2025-70936	Vtiger CRM 8.4.0 contains a reflected cross-site scripting (XSS) vulnerability in the MailManager module. Improper handling of user-controlled input in the _folder parameter allows a specially crafted, double URL-encoded payload to be reflected and executed in the context of an authenticated user s session.	5.4	More Details
CVE-2026-2712	The WP-Optimize plugin for WordPress is vulnerable to unauthorized access of functionality due to missing capability checks in the `receive_heartbeat()` function in `includes/class-wp-optimize-heartbeat.php` in all versions up to, and including, 4.5.0. This is due to the Heartbeat handler directly invoking `Updraft_Smush_Manager_Commands` methods without verifying user capabilities, nonce tokens, or the allowed commands whitelist that the normal AJAX handler (`updraft_smush_ajax`) enforces. This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke admin-only Smush operations including reading log files (`get_smush_logs`), deleting all backup images (`clean_all_backup_images`), triggering bulk image processing (`process_bulk_smush`), and modifying Smush options (`update_smush_options`).	5.4	More Details
CVE-2026-40028	Hayabusa versions prior to 3.8.0 contain a cross-site scripting (XSS) vulnerability in its HTML report output that allows an attacker to execute arbitrary JavaScript when a user scans JSON-exported logs containing malicious content in the Computer field. An attacker can inject JavaScript into the Computer field of JSON logs that executes in the forensic examiner's browser session when viewing the generated HTML report, leading to information disclosure or code execution.	5.4	More Details
CVE-2026-35207	dde-control-center is the control panel of DDE, the Deepin Desktop Environment. plugin-deepinid is a plugin in dde-control-center, which provides the deepinid cloud service. Prior to 6.1.80, plugin-deepinid is configured to skip TLS certificate verification when fetching the user's avatar from openapi.deepin.com or other providers. An MITM attacker could intercept the traffic, replace the avatar with a malicious or misleading image, and potentially identify the user by the avatar. This vulnerability is fixed in dde-control-center 6.1.80 and 5.9.9.	5.4	More Details
CVE-2025-70365	A stored cross-site scripting (XSS) vulnerability exists in Kiamo before 8.4 due to improper output encoding of user-supplied input in administrative interfaces. An authenticated administrative user can inject arbitrary JavaScript code that is executed in the browser of users viewing the affected pages.	5.4	More Details
CVE-2026-39704	Missing Authorization vulnerability in nfusionsolutions Precious Metals Automated Product Pricing – Pro precious-metals-automated-product-pricing-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Precious Metals Automated Product Pricing – Pro: from n/a through <= 4.0.5.	5.3	More Details
CVE-2026-39701	Missing Authorization vulnerability in Andrew ShopWP wpshopify allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ShopWP: from n/a through <= 5.2.4.	5.3	More Details
CVE-2026-39609	Missing Authorization vulnerability in Wava.co Wava Payment wava-payment allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wava Payment: from n/a through <= 0.3.7.	5.3	More Details
CVE-2026-39648	Missing Authorization vulnerability in themebeez Cream Blog cream-blog allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cream Blog: from n/a through <= 2.1.7.	5.3	More Details
CVE-2026-39707	Missing Authorization vulnerability in ZealousWeb Accept PayPal Payments using Contact Form 7 contact-form-7-paypal-extension allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Accept PayPal Payments using Contact Form 7: from n/a through <= 4.0.4.	5.3	More Details
CVE-2026-39637	Missing Authorization vulnerability in SpabRice Mogi mogi allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Mogi: from n/a through <= 1.2.3.	5.3	More Details
CVE-2026-	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in kutethemes Uminex uminex allows Code Injection.This issue affects Uminex: from n/a through <= 1.0.9.	5.3	More Details

39629			
CVE-2026-39706	Missing Authorization vulnerability in Netro Systems Make My Trivia trivialy allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Make My Trivia: from n/a through <= 1.1.0.	5.3	More Details
CVE-2026-39709	Insertion of Sensitive Information Into Sent Data vulnerability in thetechtribe The Tribal the-tech-tribe allows Retrieve Embedded Sensitive Data.This issue affects The Tribal: from n/a through <= 1.3.4.	5.3	More Details
CVE-2026-39608	Missing Authorization vulnerability in iPOSPays iPOSpays Gateways WC ipospays-gateways-wc allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects iPOSpays Gateways WC: from n/a through <= 1.3.7.	5.3	More Details
CVE-2026-39616	Authorization Bypass Through User-Controlled Key vulnerability in dFactory Download Attachments download-attachments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Download Attachments: from n/a through <= 1.4.0.	5.3	More Details
CVE-2026-39711	Insertion of Sensitive Information Into Sent Data vulnerability in stmcan RT-Theme 18 | Extensions rt18-extensions allows Retrieve Embedded Sensitive Data.This issue affects RT-Theme 18 | Extensions: from n/a through <= 2.5.	5.3	More Details
CVE-2026-39622	Missing Authorization vulnerability in acmethemes Education Base education-base allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Education Base: from n/a through <= 3.0.8.	5.3	More Details
CVE-2026-39712	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in tagDiv tagDiv Composer td-composer allows Code Injection.This issue affects tagDiv Composer: from n/a through <= 5.4.3.	5.3	More Details
CVE-2026-39713	Missing Authorization vulnerability in mailercloud Mailercloud – Integrate webforms and synchronize website contacts mailercloud-integrate-webforms-synchronize-contacts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Mailercloud – Integrate webforms and synchronize website contacts: from n/a through <= 1.0.7.	5.3	More Details
CVE-2026-2519	The Online Scheduling and Appointment Booking System – Bookly plugin for WordPress is vulnerable to price manipulation via the 'tips' parameter in all versions up to, and including, 27.0. This is due to the plugin trusting a user-supplied input without server-side validation against the configured price. This makes it possible for unauthenticated attackers to submit a negative number to the 'tips' parameter, causing the total price to be reduced to zero.	5.3	More Details
CVE-2026-35040	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to 6.2.1, using certain modifiers on RegExp objects in the allowedAud, allowedIss, allowedSub, allowedJti, or allowedNonce options in verify functions can cause certain unintended behaviours. This is because some modifiers are stateful and will cause failures in every second verification attempt regardless of the validity of the token provided. Such modifiers are /g (global matching) and /y (sticky matching). This does NOT allow invalid tokens to be accepted, only for valid tokens to be improperly rejected in some configurations. Instead it causes 50% of valid authentication requests to fail in an alternating pattern. This vulnerability is fixed in 6.2.1.	5.3	More Details
CVE-2026-39705	Missing Authorization vulnerability in Mulika Team MIPL WC Multisite Sync mipl-wc-multisite-sync allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MIPL WC Multisite Sync: from n/a through <= 1.4.4.	5.3	More Details
CVE-2026-39697	Missing Authorization vulnerability in HBSS Technologies MAIO – The new AI GEO / SEO tool maio-the-new-ai-geo-seo-tool allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MAIO – The new AI GEO / SEO tool: from n/a through <= 6.2.8.	5.3	More Details
CVE-2026-39624	Missing Authorization vulnerability in kutethemes Biolife biolife allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Biolife: from n/a through <= 3.2.3.	5.3	More Details
CVE-2026-39612	Missing Authorization vulnerability in kutethemes KuteShop kuteshop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects KuteShop: from n/a through <= 4.2.9.	5.3	More Details
CVE-2026-39610	Missing Authorization vulnerability in Pankaj Kumar WpXmas-Snow wpxmas-snow allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WpXmas-Snow: from n/a through <= 1.1.	5.3	More Details
CVE-2026-39714	Missing Authorization vulnerability in G5Theme G5Plus April g5plus-april allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects G5Plus April: from n/a through <= 6.8.	5.3	More Details
CVE-2026-6160	A vulnerability was found in code-projects Simple ChatBox 1.0. Affected by this issue is the function SimpleChatbox_PHP of the file chatbox.sql of the component Endpoint. Performing a manipulation results in file and directory information exposure. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	5.3	More Details

CVE-2026-39644	Missing Authorization vulnerability in Roxnor Wp Ultimate Review wp-ultimate-review allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wp Ultimate Review: from n/a through <= 2.3.8.	5.3	More Details
CVE-2026-39715	Missing Authorization vulnerability in AnyTrack AnyTrack Affiliate Link Manager anytrack-affiliate-link-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AnyTrack Affiliate Link Manager: from n/a through <= 1.5.5.	5.3	More Details
CVE-2026-39625	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in kutethemes TechOne techone allows Code Injection.This issue affects TechOne: from n/a through <= 3.0.3.	5.3	More Details
CVE-2026-39626	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in kutethemes Armania armania allows Code Injection.This issue affects Armania: from n/a through <= 1.4.8.	5.3	More Details
CVE-2026-39698	Missing Authorization vulnerability in PublisherDesk The Publisher Desk ads.txt the-publisher-desk-ads-txt allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Publisher Desk ads.txt: from n/a through <= 1.5.0.	5.3	More Details
CVE-2026-39628	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in kutethemes DukaMarket dukamarket allows Code Injection.This issue affects DukaMarket: from n/a through <= 1.3.0.	5.3	More Details
CVE-2026-39699	Missing Authorization vulnerability in massiveshift AI Workflow Automation ai-workflow-automation-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI Workflow Automation: from n/a through <= 1.4.2.	5.3	More Details
CVE-2026-39716	Missing Authorization vulnerability in CKThemes Flipmart flipmart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flipmart: from n/a through <= 2.8.	5.3	More Details
CVE-2026-39643	Missing Authorization vulnerability in Payment Plugins Payment Plugins for PayPal WooCommerce pymntpl-paypal-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Payment Plugins for PayPal WooCommerce: from n/a through <= 2.0.13.	5.3	More Details
CVE-2026-39536	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in WP Chill RSVP and Event Management rsvp allows Retrieve Embedded Sensitive Data.This issue affects RSVP and Event Management: from n/a through <= 2.7.16.	5.3	More Details
CVE-2026-39694	Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.10.2.	5.3	More Details
CVE-2026-39672	Missing Authorization vulnerability in shiptime ShipTime: Discounted Shipping Rates shiptime-discount-shipping allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ShipTime: Discounted Shipping Rates: from n/a through <= 1.1.1.	5.3	More Details
CVE-2026-40087	LangChain is a framework for building agents and LLM-powered applications. Prior to 0.3.84 and 1.2.28, LangChain's f-string prompt-template validation was incomplete in two respects. First, some prompt template classes accepted f-string templates and formatted them without enforcing the same attribute-access validation as PromptTemplate. In particular, DictPromptTemplate and ImagePromptTemplate could accept templates containing attribute access or indexing expressions and subsequently evaluate those expressions during formatting. Second, f-string validation based on parsed top-level field names did not reject nested replacement fields inside format specifiers. In this pattern, the nested replacement field appears in the format specifier rather than in the top-level field name. As a result, earlier validation based on parsed field names did not reject the template even though Python formatting would still attempt to resolve the nested expression at runtime. This vulnerability is fixed in 0.3.84 and 1.2.28.	5.3	More Details
CVE-2026-39882	OpenTelemetry-Go is the Go implementation of OpenTelemetry. Prior to 1.43.0, the otlp HTTP exporters (traces/metrics/logs) read the full HTTP response body into an in-memory bytes.Buffer without a size cap. This is exploitable for memory exhaustion when the configured collector endpoint is attacker-controlled (or a network attacker can mitm the exporter connection). This vulnerability is fixed in 1.43.0.	5.3	More Details
CVE-2026-5083	Ado::Sessions versions through 0.935 for Perl generates insecure session ids. The session id is generated from a SHA-1 hash seeded with the built-in rand function, the epoch time, and the PID. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems. Note that Ado is no longer maintained, and has been removed from the CPAN index. It is still available on BackPAN.	5.3	More Details
CVE-2026-39656	Missing Authorization vulnerability in Razorpay Razorpay for WooCommerce woo-razorpay allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Razorpay for WooCommerce: from n/a through <= 4.8.2.	5.3	More Details
CVE-2026-39669	Missing Authorization vulnerability in NitroPack NitroPack nitropack allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects NitroPack: from n/a through <= 1.19.3.	5.3	More Details

CVE-2026-5082	Amon2::Plugin::Web::CSRFDefender versions from 7.00 through 7.03 for Perl generate an insecure session id. The generate_session_id function will attempt to read bytes from the /dev/urandom device, but if that is unavailable then it generates bytes using SHA-1 hash seeded with the built-in rand() function, the PID, and the high resolution epoch time. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Amon2::Plugin::Web::CSRFDefender versions before 7.00 were part of Amon2, which was vulnerable to insecure session ids due to CVE-2025-15604. Note that the author has deprecated this module.	5.3	More Details
CVE-2026-39473	Insertion of Sensitive Information Into Sent Data vulnerability in Pär Thernström Simple History simple-history allows Retrieve Embedded Sensitive Data.This issue affects Simple History: from n/a through <= 5.24.0.	5.3	More Details
CVE-2026-39412	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.25.4, the sort_natural filter bypasses the ownPropertyOnly security option, allowing template authors to extract values of prototype-inherited properties through a sorting side-channel attack. Applications relying on ownPropertyOnly: true as a security boundary (e.g., multi-tenant template systems) are exposed to information disclosure of sensitive prototype properties such as API keys and tokens. This vulnerability is fixed in 10.25.4.	5.3	More Details
CVE-2026-2263	The Hustle – Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'hustle_module_converted' AJAX action in all versions up to, and including, 7.8.10.2. This makes it possible for unauthenticated attackers to forge conversion tracking events for any Hustle module, including draft modules that are never displayed to users, thereby manipulating marketing analytics and conversion statistics.	5.3	More Details
CVE-2026-32990	Improper Input Validation vulnerability in Apache Tomcat due to an incomplete fix of CVE-2025-66614. This issue affects Apache Tomcat: from 11.0.15 through 11.0.19, from 10.1.50 through 10.1.52, from 9.0.113 through 9.0.115. Users are recommended to upgrade to version 11.0.20, 10.1.53 or 9.0.116, which fix the issue.	5.3	More Details
CVE-2026-35665	OpenClaw before 2026.3.24 contains an incomplete fix for CVE-2026-32011 where the Feishu webhook handler accepts request bodies with permissive limits of 1MB and 30-second timeout before signature verification. An unauthenticated attacker can exhaust server connection resources by sending concurrent slow HTTP POST requests to the Feishu webhook endpoint, blocking legitimate webhook deliveries.	5.3	More Details
CVE-2026-22560	An open redirect vulnerability in Rocket.Chat versions prior to 8.4.0 allows users to be redirected to arbitrary URLs by manipulating parameters within a SAML endpoint.	5.3	More Details
CVE-2026-6219	A vulnerability was determined in aandrew-me ytDownloader up to 3.20.2. This affects the function child_process.exec of the file src/compressor.js of the component Compressor Feature. This manipulation causes command injection. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	5.3	More Details
CVE-2026-39673	Missing Authorization vulnerability in shrikantkale iZooto izooto-web-push allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects iZooto: from n/a through <= 3.7.20.	5.3	More Details
CVE-2026-35647	OpenClaw before 2026.3.25 contains an access control vulnerability where verification notices bypass DM policy checks and reply to unpaired peers. Attackers can send verification notices to users outside allowed direct message policies by exploiting insufficient access validation before message transmission.	5.3	More Details
CVE-2026-33899	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below 7.1.2-189 and 6.9.13-44, when `Magick` parses an XML file it is possible that a single zero byte is written out of the bounds. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.3	More Details
CVE-2026-39501	Missing Authorization vulnerability in RealMag777 FOX woocommerce-currency-switcher allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FOX: from n/a through <= 1.4.5.	5.3	More Details
CVE-2026-35654	OpenClaw before 2026.3.25 contains an authorization bypass vulnerability in Microsoft Teams feedback invokes that allows unauthorized senders to record session feedback. Attackers can bypass sender allowlist checks via feedback invoke endpoints to trigger unauthorized feedback recording or reflection.	5.3	More Details
CVE-2026-35661	OpenClaw before 2026.3.25 contains an authorization bypass vulnerability in Telegram callback query handling that allows attackers to mutate session state without satisfying normal DM pairing requirements. Remote attackers can exploit weaker callback-only authorization in direct messages to bypass DM pairing and modify session state.	5.3	More Details
CVE-2026-39606	Missing Authorization vulnerability in Foysal Imran BizReview bizreview allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BizReview: from n/a through <= 1.5.13.	5.3	More Details
CVE-2026-4654	The Awesome Support – WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 6.3.7. This is due to the wpas_get_ticket_replies_ajax() function failing to verify whether the authenticated user has permission to view the specific ticket being requested. This makes it possible for authenticated attackers, with subscriber-level access and above, to access sensitive information from all support tickets in the system by manipulating the ticket_id parameter.	5.3	More Details
	A flaw has been found in zhayujie chatgpt-on-wechat CowAgent up to 2.0.4. This affects the function dispatch of the		

CVE-2026-5998	file agent/memory/service.py of the component API Memory Content Endpoint. This manipulation of the argument filename causes path traversal. The attack can be initiated remotely. The exploit has been published and may be used. Upgrading to version 2.0.5 mitigates this issue. Patch name: 174ee0cafc9e8e9d97a23c305418251485b8aa89. It is recommended 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.	5.3	More Details
CVE-2026-4664	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 5.103.0. This is due to the `create_review_permissions_check()` function comparing the user-supplied `key` parameter against the order's `ivole_secret_key` meta value using strict equality (`===`), without verifying that the stored key is non-empty. For orders where no review reminder email has been sent, the `ivole_secret_key` meta is not set, causing `get_meta()` to return an empty string. An attacker can supply `key: ""` to match this empty value and bypass the permission check. This makes it possible for unauthenticated attackers to submit, modify, and inject product reviews on any product — including products not associated with the referenced order — via the REST API endpoint `POST /ivole/v1/review`. Reviews are auto-approved by default since `ivole_enable_moderation` defaults to `"no"`.	5.3	More Details
CVE-2026-34069	nimiq/core-rs-albatross is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. In versions 1.2.2 and below, an unauthenticated p2p peer can cause the RequestMacroChain message handler task to panic. Sending a RequestMacroChain message where the first locator hash on the victim's main chain is a micro block hash (not a macro block hash) causes said panic. The RequestMacroChain::handle handler selects the locator based only on "is on main chain", then calls get_macro_blocks() and panics via .unwrap() when the selected hash is not a macro block (BlockchainError::BlockIsNotMacro). This issue has been fixed in version 1.3.0.	5.3	More Details
CVE-2026-3477	The PZ Frontend Manager plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 1.0.6. The pzfm_user_request_action_callback() function, registered via the wp_ajax_pzfm_user_request_action action hook, lacks both capability checks and nonce verification. This function handles user activation, deactivation, and deletion operations. When the 'dataType' parameter is set to 'delete', the function calls wp_delete_user() on all provided user IDs without verifying that the current user has the appropriate permissions. Notably, the similar pzfm_remove_item_callback() function does check pzfm_can_delete_user() before performing deletions, indicating this was an oversight. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary WordPress users (including administrators) by sending a crafted request to the AJAX endpoint.	5.3	More Details
CVE-2026-31924	Cleartext Transmission of Sensitive Information vulnerability in Apache APISIX. tencent-cloud-cls log export uses plaintext HTTP This issue affects Apache APISIX: from 2.99.0 through 3.15.0. Users are recommended to upgrade to version 3.16.0, which fixes the issue.	5.3	More Details
CVE-2026-39658	Missing Authorization vulnerability in Coding Panda Panda Pods Repeater Field panda-pods-repeater-field allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Panda Pods Repeater Field: from n/a through <= 1.5.12.	5.3	More Details
CVE-2026-39657	Missing Authorization vulnerability in leadlovers leadlovers forms leadlovers-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects leadlovers forms: from n/a through <= 1.0.2.	5.3	More Details
CVE-2026-39659	Missing Authorization vulnerability in Ultimate Member Ultimate Member ultimate-member allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Member: from n/a through <= 2.11.3.	5.3	More Details
CVE-2026-39660	Missing Authorization vulnerability in Automattic WP Job Manager wp-job-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Manager: from n/a through <= 2.4.1.	5.3	More Details
CVE-2026-39662	Missing Authorization vulnerability in ProWCPlugins Product Price by Formula for WooCommerce product-price-by-formula-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Product Price by Formula for WooCommerce: from n/a through <= 2.5.6.	5.3	More Details
CVE-2026-35626	OpenClaw before 2026.3.22 contains an unauthenticated resource exhaustion vulnerability in voice call webhook handling that buffers request bodies before provider signature checks. Attackers can send large or malicious webhook requests to exhaust server resources without authentication by bypassing signature validation.	5.3	More Details
CVE-2026-39663	Missing Authorization vulnerability in themetechmount TrueBooker truebooker-appointment-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects TrueBooker: from n/a through <= 1.1.5.	5.3	More Details
CVE-2026-35633	OpenClaw before 2026.3.22 contains an unbounded memory allocation vulnerability in remote media HTTP error handling that allows attackers to trigger excessive memory consumption. Attackers can send crafted HTTP error responses with large bodies to remote media endpoints, causing the application to allocate unbounded memory before failure handling occurs.	5.3	More Details
CVE-2026-39664	Missing Authorization vulnerability in leadrebel Leadrebel leadrebel allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Leadrebel: from n/a through <= 1.0.2.	5.3	More Details
CVE-2026-	Out of bounds read in WebAudio in Google Chrome on Mac prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity:	5.3	More Details

5886	Medium)		
CVE-2026-35640	OpenClaw before 2026.3.25 parses JSON request bodies before validating webhook signatures, allowing unauthenticated attackers to force resource-intensive parsing operations. Remote attackers can send malicious webhook requests to trigger denial of service by exhausting server resources through forced JSON parsing before signature rejection.	5.3	More Details
CVE-2026-3594	The Riaxe Product Customizer plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.4 via the '/wp-json/InkXEProductDesignerLite/orders' REST API endpoint. The endpoint is registered with 'permission_callback' set to '__return_true', meaning no authentication or authorization checks are performed. The endpoint queries WooCommerce order data from the database and returns it to the requester, including customer first and last names, customer IDs, order IDs, order totals, order dates, currencies, and order statuses. This makes it possible for unauthenticated attackers to extract sensitive customer and order information from the WooCommerce store.	5.3	More Details
CVE-2026-40151	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the AgentOS deployment platform exposes a GET /api/agents endpoint that returns agent names, roles, and the first 100 characters of agent system instructions to any unauthenticated caller. The AgentOS FastAPI application has no authentication middleware, no API key validation, and defaults to CORS allow_origins=["*"] with host="0.0.0.0", making every deployment network-accessible and queryable from any origin by default. This vulnerability is fixed in 4.5.128.	5.3	More Details
CVE-2026-40152	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, he list_files() tool in FileTools validates the directory parameter against workspace boundaries via _validate_path(), but passes the pattern parameter directly to Path.glob() without any validation. Since Python's Path.glob() supports .. path segments, an attacker can use relative path traversal in the glob pattern to enumerate arbitrary files outside the workspace, obtaining file metadata (existence, name, size, timestamps) for any path on the filesystem. This vulnerability is fixed in 1.5.128.	5.3	More Details
CVE-2026-5167	The Masteriyo LMS – Online Course Builder for eLearning, LMS & Education plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in versions up to and including 2.1.7. This is due to insufficient webhook signature verification in the handle_webhook() function. The webhook endpoint processes unauthenticated requests and only performs signature verification if both the webhook_secret setting is configured AND the HTTP_STRIPE_SIGNATURE header is present. Since webhook_secret defaults to an empty string, the webhook processes attacker-controlled JSON payloads without any verification. This makes it possible for unauthenticated attackers to send fake Stripe webhook events with arbitrary order_id values in the metadata, mark any order as completed without payment, and gain unauthorized access to paid course content.	5.3	More Details
CVE-2026-5986	A weakness has been identified in Zod jsVideoUrlParser up to 0.5.1. The impacted element is the function getTime in the library lib/util.js. This manipulation of the argument timestamp causes inefficient regular expression complexity. It is possible to initiate the attack 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.	5.3	More Details
CVE-2026-39668	Missing Authorization vulnerability in g5theme Book Previewer for Woocommerce book-previewer-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Book Previewer for Woocommerce: from n/a through <= 1.0.6.	5.3	More Details
CVE-2026-35664	OpenClaw before 2026.3.25 contains an authentication bypass vulnerability in raw card send surface that allows unpaired recipients to mint legacy callback payloads. Attackers can send raw card commands to bypass DM pairing restrictions and reach callback handling without proper authorization.	5.3	More Details
CVE-2026-39700	Missing Authorization vulnerability in WPXPO WowOptin optin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WowOptin: from n/a through <= 1.4.32.	5.3	More Details
CVE-2026-39505	Missing Authorization vulnerability in Craig Hewitt Seriously Simple Podcasting seriously-simple-podcasting allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Seriously Simple Podcasting: from n/a through <= 3.14.2.	5.3	More Details
CVE-2026-39585	Missing Authorization vulnerability in Arraytics Booktics booktics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booktics: from n/a through <= 1.0.16.	5.3	More Details
CVE-2026-39509	Missing Authorization vulnerability in wpWax Directorist directorist allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Directorist: from n/a through <= 8.5.10.	5.3	More Details
CVE-2026-39682	Missing Authorization vulnerability in Arjan Pronk linkPizza-Manager linkpizza-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects linkPizza-Manager: from n/a through <= 5.5.5.	5.3	More Details
CVE-2026-39570	Insertion of Sensitive Information Into Sent Data vulnerability in AA Web Servant 12 Step Meeting List 12-step-meeting-list allows Retrieve Embedded Sensitive Data.This issue affects 12 Step Meeting List: from n/a through <= 3.19.9.	5.3	More Details
CVE-2026-39571	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Themefic Instantio instantio allows Retrieve Embedded Sensitive Data.This issue affects Instantio: from n/a through <= 3.3.30.	5.3	More Details

CVE-2026-39685	Missing Authorization vulnerability in Ivaudore The Moneytizer the-moneytizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Moneytizer: from n/a through <= 10.0.10.	5.3	More Details
CVE-2026-39652	Missing Authorization vulnerability in igms iGMS Direct Booking igms-direct-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects iGMS Direct Booking: from n/a through <= 1.3.	5.3	More Details
CVE-2026-39687	Missing Authorization vulnerability in Rapid Car Check Rapid Car Check Vehicle Data free-vehicle-data-uk allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Rapid Car Check Vehicle Data: from n/a through <= 2.0.	5.3	More Details
CVE-2026-39688	Missing Authorization vulnerability in Glowlogix WP Frontend Profile wp-front-end-profile allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Frontend Profile: from n/a through <= 1.3.9.	5.3	More Details
CVE-2025-14243	A flaw was found in the OpenShift Mirror Registry. This vulnerability allows an unauthenticated, remote attacker to enumerate valid usernames and email addresses via different error messages during authentication failures and account creation.	5.3	More Details
CVE-2026-39586	Insertion of Sensitive Information Into Sent Data vulnerability in Ateeq Rafeeq RepairBuddy computer-repair-shop allows Retrieve Embedded Sensitive Data.This issue affects RepairBuddy: from n/a through <= 4.1132.	5.3	More Details
CVE-2026-39563	Missing Authorization vulnerability in ILLID Share This Image share-this-image allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Share This Image: from n/a through <= 2.12.	5.3	More Details
CVE-2026-39588	Missing Authorization vulnerability in nmerii NM Gift Registry and Wishlist Lite nm-gift-registry-and-wishlist-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects NM Gift Registry and Wishlist Lite: from n/a through <= 5.13.	5.3	More Details
CVE-2026-39407	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.12, a path handling inconsistency in serveStatic allows protected static files to be accessed by using repeated slashes (//) in the request path. When route-based middleware (e.g., /admin/*) is used for authorization, the router may not match paths containing repeated slashes, while serveStatic resolves them as normalized paths. This can lead to a middleware bypass. This vulnerability is fixed in 4.12.12.	5.3	More Details
CVE-2026-39406	@hono/node-server allows running the Hono application on Node.js. Prior to 1.19.13, a path handling inconsistency in serveStatic allows protected static files to be accessed by using repeated slashes (//) in the request path. When route-based middleware (e.g., /admin/*) is used for authorization, the router may not match paths containing repeated slashes, while serveStatic resolves them as normalized paths. This can lead to a middleware bypass. This vulnerability is fixed in 1.19.13.	5.3	More Details
CVE-2026-39650	Missing Authorization vulnerability in Unitech Web UnitechPay unitechpay-paiements-mobile-money allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UnitechPay: from n/a through <= 1.0.2.	5.3	More Details
CVE-2026-5833	A security vulnerability has been detected in awwaiid mcp-server-taskwarrior up to 1.0.1. This impacts the function server.setRequestHandler of the file index.ts. Such manipulation of the argument Identifier leads to command injection. The attack must be carried out locally. The exploit has been disclosed publicly and may be used. The name of the patch is 1ee3d282debfa0a99afeb41d22c4b2fd5a3148f2. Applying a patch is advised to resolve this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	5.3	More Details
CVE-2026-39690	Missing Authorization vulnerability in Paul Bearne Author Avatars List/Block author-avatars allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Author Avatars List/Block: from n/a through <= 2.1.25.	5.3	More Details
CVE-2026-39649	Missing Authorization vulnerability in themebeez Royale News royale-news allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Royale News: from n/a through <= 2.2.4.	5.3	More Details
CVE-2026-39691	Missing Authorization vulnerability in AdAstraCrypto Cryptocurrency Donation Box – Bitcoin & Crypto Donations cryptocurrency-donation-box allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cryptocurrency Donation Box – Bitcoin & Crypto Donations: from n/a through <= 2.2.13.	5.3	More Details
CVE-2026-39605	Missing Authorization vulnerability in Obadiah Super Custom Login super-custom-login allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Super Custom Login: from n/a through <= 1.1.	5.3	More Details
CVE-2026-39564	Insertion of Sensitive Information Into Sent Data vulnerability in sunshinephotocart Sunshine Photo Cart sunshine-photo-cart allows Retrieve Embedded Sensitive Data.This issue affects Sunshine Photo Cart: from n/a through < 3.6.2.	5.3	More Details
CVE-2026-	Missing Authorization vulnerability in MWP Development Diet Calorie Calculator diet-calorie-calculator allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Diet Calorie Calculator: from n/a	5.3	More Details

39680	through <= 1.1.1.		
CVE-2026-39562	Missing Authorization vulnerability in BoldGrid Client Invoicing by Sprout Invoices sprout-invoices allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Client Invoicing by Sprout Invoices: from n/a through <= 20.8.10.	5.3	More Details
CVE-2026-39520	Missing Authorization vulnerability in weDevs weDocs wedocs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects weDocs: from n/a through <= 2.1.18.	5.3	More Details
CVE-2026-39535	Missing Authorization vulnerability in fullworks Display Eventbrite Events widget-for-eventbrite-api allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Display Eventbrite Events: from n/a through <= 6.5.6.	5.3	More Details
CVE-2025-15565	The Nexi XPay plugin for WordPress is vulnerable to unauthorized modification of data due to missing authorization checks on the redirect function in all versions up to, and including, 8.3.0. This makes it possible for unauthenticated attackers to mark pending WooCommerce orders as paid/completed.	5.3	More Details
CVE-2026-33705	Chamilo LMS is a learning management system. Prior to 1.11.38, Twig template files (.tpl) under /main/template/default/ are directly accessible without authentication via HTTP GET requests. These templates expose internal application logic, variable names, AJAX endpoint URLs, and admin panel structure. This vulnerability is fixed in 1.11.38.	5.3	More Details
CVE-2026-4299	The MainWP Child Reports plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 2.2.6. This is due to a missing capability check in the heartbeat_received() function in the Live_Update class. This makes it possible for authenticated attackers, with Subscriber-level access and above, to obtain MainWP Child Reports activity log entries (including action summaries, user information, IP addresses, and contextual data) via the WordPress Heartbeat API by sending a crafted heartbeat request with the 'wp-mainwp-stream-heartbeat' data key.	5.3	More Details
CVE-2026-40100	FastGPT is an AI Agent building platform. Prior to 4.14.10.3, the /api/core/app/mcpTools/runTool endpoint accepts arbitrary URLs without authentication. The internal IP check in isInternalAddress() only blocks private IPs when CHECK_INTERNAL_IP=true, which is not the default. This allows unauthenticated attackers to perform SSRF against internal network resources. This vulnerability is fixed in 4.14.10.3.	5.3	More Details
CVE-2026-3646	The LTL Freight Quotes – R+L Carriers Edition plugin for WordPress is vulnerable to Missing Authorization via the plugin's webhook handler in all versions up to, and including, 3.3.13. This is due to missing authentication, authorization, and nonce verification on a standalone PHP file that directly processes GET parameters and updates WordPress options. This makes it possible for unauthenticated attackers to modify the plugin's subscription plan settings, effectively downgrading the store from a paid plan to the Trial Plan, changing the store type, and manipulating subscription expiration dates, potentially disabling premium features such as Dropship and Hazardous Material handling.	5.3	More Details
CVE-2026-33737	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, multiple files use simplexml_load_string() without XXE protection. With LIBXML_NOENT flag, arbitrary server files can be read. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	5.3	More Details
CVE-2026-39675	Missing Authorization vulnerability in webmuehle Court Reservation court-reservation allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Court Reservation: from n/a through <= 1.10.11.	5.3	More Details
CVE-2026-39542	Insertion of Sensitive Information Into Sent Data vulnerability in Doofinder Doofinder for WooCommerce doofinder-for-woocommerce allows Retrieve Embedded Sensitive Data.This issue affects Doofinder for WooCommerce: from n/a through <= 2.10.13.	5.3	More Details
CVE-2026-39543	Missing Authorization vulnerability in Themefic Tourfic tourfic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tourfic: from n/a through <= 2.21.4.	5.3	More Details
CVE-2026-39561	Missing Authorization vulnerability in WP Chill Revive.so revive-so allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Revive.so: from n/a through <= 2.0.7.	5.3	More Details
CVE-2026-40086	Rembg is a tool to remove images background. Prior to 2.0.75, a path traversal vulnerability in the rembg HTTP server allows unauthenticated remote attackers to read arbitrary files from the server's filesystem. By sending a crafted request with a malicious model_path parameter, an attacker can force the server to attempt loading any file as an ONNX model, revealing file existence, permissions, and potentially file contents through error messages. This vulnerability is fixed in 2.0.75.	5.3	More Details
CVE-2026-39676	Missing Authorization vulnerability in Shahjada Download Manager download-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Download Manager: from n/a through <= 3.3.52.	5.3	More Details
CVE-2026-39516	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in POSIMYTH Nexter Blocks the-plus-addons-for-block-editor allows Retrieve Embedded Sensitive Data.This issue affects Nexter Blocks: from n/a through <= 4.7.0.	5.3	More Details
CVE-2026-	Missing Authorization vulnerability in DOTonPAPER Pinpoint Booking System booking-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Pinpoint Booking System: from n/a through	5.3	More

39678	<= 2.9.9.6.5.		Details
CVE-2026-39528	Missing Authorization vulnerability in WP Delicious WP Delicious delicious-recipes allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Delicious: from n/a through <= 1.9.5.	5.3	More Details
CVE-2026-32591	A flaw was found in Red Hat Quay's Proxy Cache configuration feature. When an organization administrator configures an upstream registry for proxy caching, Quay makes a network connection to the specified registry hostname without verifying that it points to a legitimate external service. An attacker with organization administrator privileges could supply a crafted hostname to force the Quay server to make requests to internal network services, cloud infrastructure endpoints, or other resources that should not be accessible from the Quay application.	5.2	More Details
CVE-2026-40447	Integer overflow or wraparound vulnerability in Samsung Open Source Escargot allows undefined behavior.This issue affects Escargot: 97e8115ab1110bc502b4b5e4a0c689a71520d335.	5.1	More Details
CVE-2026-34238	ImageMagick is free and open-source software used for editing and manipulating digital images. In versions below both 7.1.2-19 and 6.9.13-44, an integer overflow in the despeckle operation causes a heap buffer overflow on 32-bit builds that will result in an out of bounds write. This issue has been fixed in versions 6.9.13-44 and 7.1.2-19.	5.1	More Details
CVE-2026-35634	OpenClaw before 2026.3.23 contains an authentication bypass vulnerability in the Canvas gateway where authorizeCanvasRequest() unconditionally allows local-direct requests without validating bearer tokens or canvas capabilities. Attackers can send unauthenticated loopback HTTP and WebSocket requests to Canvas routes to bypass authentication and gain unauthorized access.	5.1	More Details
CVE-2026-34757	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From 1.0.9 to before 1.6.57, passing a pointer obtained from png_get_PLTE, png_get_tRNS, or png_get_hIST back into the corresponding setter on the same png_struct/png_info pair causes the setter to read from freed memory and copy its contents into the replacement buffer. The setter frees the internal buffer before copying from the caller-supplied pointer, which now dangles. The freed region may contain stale data (producing silently corrupted chunk metadata) or data from subsequent heap allocations (leaking unrelated heap contents into the chunk struct). This vulnerability is fixed in 1.6.57.	5.1	More Details
CVE-2026-34866	Out-of-bounds write vulnerability in the WEB module.Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	5.1	More Details
CVE-2026-39418	MaxKB is an open-source AI assistant for enterprise. In versions 2.7.1 and below, sandbox network protection can be bypassed by using socket.sendto() with the MSG_FASTOPEN flag. This allows authenticated user with tool-editing permissions to reach internal services that are explicitly blocked by the sandbox's banned hosts configuration. MaxKB's sandbox uses LD_PRELOAD to hook the connect() function and block connections to banned IPs, but Linux's sendto() with the MSG_FASTOPEN flag can establish TCP connections directly through the kernel without ever calling connect(), completely bypassing the IP validation. Although sendto is listed in the syscall() wrapper, this is ineffective because glibc invokes the kernel syscall directly rather than routing through the hooked syscall() function. This issue has been fixed in version 2.8.0.	5.0	More Details
CVE-2026-34262	Information Disclosure Vulnerability in SAP HANA Cockpit and HANA Database Explorer	5.0	More Details
CVE-2026-4979	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to blind Server-Side Request Forgery in all versions up to, and including, 1.2.58. This is due to insufficient URL origin validation in the process_image_crop() method when processing avatar/banner image crop operations. The function accepts a user-controlled URL via the uwp_crop POST parameter and only validates it using esc_url() for sanitization and wp_check_filetype() for extension verification, without enforcing that the URL references a local uploads file. The URL is then passed to uwp_resizeThumbnailImage() which uses it in PHP image processing functions (getimagesize(), imagecreatefrom*()) that support URL wrappers and perform outbound HTTP requests. This makes it possible for authenticated attackers with subscriber-level access and above to coerce the WordPress server into making arbitrary HTTP requests to attacker-controlled or internal network destinations, enabling internal network scanning and potential access to sensitive services.	5.0	More Details
CVE-2026-39411	LobeHub is a work-and-lifestyle space to find, build, and collaborate with agent teammates that grow with you. Prior to 2.1.48, the webapi authentication layer trusts a client-controlled X-lobe-chat-auth header that is only XOR-obfuscated, not signed or otherwise authenticated. Because the XOR key is hardcoded in the repository, an attacker can forge arbitrary auth payloads and bypass authentication on protected webapi routes. Affected routes include /webapi/chat/[provider], /webapi/models/[provider], /webapi/models/[provider]/pull, and /webapi/create-image/comfyui. This vulnerability is fixed in 2.1.48.	5.0	More Details
CVE-2026-39880	Remnawave Backend is the backend for the Remnawave proxy and user management solution. Prior to 2.7.5, a glitch in the HWID device registration logic allows an authenticated user to bypass the configured limit for HWID devices and register more devices than expected, allowing them to resell subscriptions and consume excessive traffic. This vulnerability is fixed in 2.7.5.	5.0	More Details
CVE-2026-	Vim is an open source, command line text editor. Prior to 9.2.0316, a command injection vulnerability in Vim's netbeans interface allows a malicious netbeans server to execute arbitrary Ex commands when Vim connects to it,	5.0	More

39881	via unsanitized strings in the defineAnnoType and specialKeys protocol messages. This vulnerability is fixed in 9.2.0316.		Details
CVE-2026-25125	October is a Content Management System (CMS) and web platform. Versions prior to 3.7.14 and 4.1.10 contain a server-side information disclosure vulnerability in the INI settings parser. Because PHP's parse_ini_string() function supports ${} syntax for environment variable interpolation, attackers with Editor access could inject patterns such as ${APP_KEY} or ${DB_PASSWORD} into CMS page settings fields, causing sensitive environment variables to be resolved, stored in the template, and returned to the attacker when the page was reopened. This could enable exfiltration of credentials and secrets (database passwords, AWS keys, application keys), potentially leading to further attacks such as database access or cookie forgery. The vulnerability is only relevant when cms.safe_mode is enabled, as direct PHP injection is already possible otherwise. This issue has been fixed in versions 3.7.14 and 4.1.10. If users are unable to immediately upgrade, they can workaround this issue by restricting Editor tool access to fully trusted administrators only, and ensuring database and cloud service credentials are not accessible from the web server's network.	4.9	More Details
CVE-2026-27673	Due to a missing authorization check, SAP S/4HANA (Private Cloud and On-Premise) allows an authenticated user to delete files on the operating system and gain unauthorized control over file operations which could leads to no impact on Confidentiality, Low impact on Integrity and Availability of the application.	4.9	More Details
CVE-2026-22692	October is a Content Management System (CMS) and web platform. Versions prior to 3.7.13 and versions 4.0.0 through 4.1.4 contain a sandbox bypass vulnerability in the optional Twig safe mode feature (CMS_SAFE_MODE). Certain methods on the collect() helper were not properly restricted, allowing authenticated users with template editing permissions to bypass sandbox protections. Exploitation requires authenticated backend access with CMS template editing permissions and only affects installations with CMS_SAFE_MODE enabled (disabled by default). This issue has been fixed in versions 3.7.13 and 4.1.5. To workaround this issue, users can disable CMS_SAFE_MODE if untrusted template editing is not required, and restrict CMS template editing permissions to fully trusted administrators only.	4.9	More Details
CVE-2026-39631	Missing Authorization vulnerability in Ronik@UnlimitedWP WPSchoolPress wpschoolpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPSchoolPress: from n/a through <= 2.2.35.	4.9	More Details
CVE-2026-39521	Server-Side Request Forgery (SSRF) vulnerability in Nelio Software Nelio Content nelio-content allows Server Side Request Forgery.This issue affects Nelio Content: from n/a through <= 4.3.1.	4.9	More Details
CVE-2026-39811	A integer overflow or wraparound vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4 all versions, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow attacker to denial of service via <insert attack vector here>	4.9	More Details
CVE-2026-35623	OpenClaw before 2026.3.25 contains a missing rate limiting vulnerability in webhook authentication that allows attackers to brute-force weak webhook passwords without throttling. Remote attackers can repeatedly submit incorrect password guesses to the webhook endpoint to compromise authentication and gain unauthorized access.	4.8	More Details
CVE-2026-35635	OpenClaw before 2026.3.22 contains a webhook path route replacement vulnerability in the Synology Chat extension that allows attackers to collapse multi-account configurations onto shared webhook paths. Attackers can exploit inherited or duplicate webhook paths to bypass per-account DM access control policies and replace route ownership across accounts.	4.8	More Details
CVE-2026-39812	A improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox PaaS 5.0.0 through 5.0.5, FortiSandbox PaaS 4.4.0 through 4.4.8, FortiSandbox PaaS 4.2 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here>	4.8	More Details
CVE-2026-39391	CI4MS is a CodeIgniter 4-based CMS skeleton that delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to 0.31.4.0, the blacklist (ban) note parameter in UserController::ajax_blackList_post() is stored in the database without sanitization and rendered into an HTML data-note attribute without escaping. An admin with blacklist privileges can inject arbitrary JavaScript that executes in the browser of any other admin who views the user management page. This vulnerability is fixed in 0.31.4.0.	4.8	More Details
CVE-2026-35628	OpenClaw before 2026.3.25 contains a missing rate limiting vulnerability in Telegram webhook authentication that allows attackers to brute-force weak webhook secrets. The vulnerability enables repeated authentication guesses without throttling, permitting attackers to systematically guess webhook secrets through brute-force attacks.	4.8	More Details
CVE-2026-35646	OpenClaw before 2026.3.25 contains a pre-authentication rate-limit bypass vulnerability in webhook token validation that allows attackers to brute-force weak webhook secrets. The vulnerability exists because invalid webhook tokens are rejected without throttling repeated authentication attempts, enabling attackers to guess weak tokens through rapid successive requests.	4.8	More Details
CVE-2026-39410	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.12, a discrepancy between browser cookie parsing and parse() handling allows cookie prefix protections to be bypassed. Cookie names that are treated as distinct by the browser may be normalized to the same key by parse(), allowing attacker-controlled cookies to override legitimate ones. This vulnerability is fixed in 4.12.12.	4.8	More Details
	The Gravity Forms plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `form_ids` parameter in the `gform_get_config` AJAX action in all versions up to, and including, 2.9.30. This is due to the `GFCommon::send_json()` method outputting JSON-encoded data wrapped in HTML comment delimiters using `echo`		

CVE-2026-4406	and `wp_die()`, which serves the response with a `Content-Type: text/html` header instead of `application/json`. The `wp_json_encode()` function does not HTML-encode angle brackets within JSON string values, allowing injected HTML/script tags in `form_ids` array values to be parsed and executed by the browser. The required `config_nonce` is generated with `wp_create_nonce('gform_config_ajax')` and is publicly embedded on every page that renders a Gravity Forms form, making it identical for all unauthenticated visitors within the same 12-hour nonce tick. 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. This vulnerability cannot be exploited against users who are authenticated on the target system, but could be used to alter the target page.	4.7	More Details
CVE-2026-5848	A vulnerability was found in jeecgboot JimuReport up to 2.3.0. The affected element is the function DriverManager.getConnection of the file /drag/onlDragDataSource/testConnection of the component Data Source Handler. Performing a manipulation of the argument dbUrl results in code injection. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor confirmed the issue and will provide a fix in the upcoming release.	4.7	More Details
CVE-2026-32932	Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an Open Redirect vulnerability in the session course edit page allows an attacker to redirect an authenticated administrator to an arbitrary external URL after saving coach assignment changes. The redirect also leaks the id_session parameter to the attacker's server. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3.	4.7	More Details
CVE-2026-40223	In systemd 258 before 260, a local unprivileged user can trigger an assert when a Delegate=yes and User=<unset> unit exists and is running.	4.7	More Details
CVE-2026-39484	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in John Darrel Hide My WP Ghost hide-my-wp allows Phishing.This issue affects Hide My WP Ghost: from n/a through < 7.0.00.	4.7	More Details
CVE-2026-5987	A security vulnerability has been detected in Sanluan PublicCMS up to 6.202506.d. This affects the function AbstractFreemarkerView.doRender of the file publiccms-parent/publiccms-core/src/main/java/com/publiccms/common/base/AbstractFreemarkerView.java of the component FreeMarker Template Handler. Such manipulation leads to improper neutralization of special elements used in a template engine. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-5838	A vulnerability was determined in PHPGurukul News Portal Project 4.1. This vulnerability affects unknown code of the file /admin/add-subadmins.php. This manipulation of the argument sadminusername causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-5839	A vulnerability was identified in PHPGurukul News Portal Project 4.1. This issue affects some unknown processing of the file /admin/add-subcategory.php. Such manipulation of the argument sucatdescription leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-6220	A vulnerability was identified in HummerRisk up to 1.5.0. This vulnerability affects the function ServerService.addServer of the file ServerService.java of the component Video File Download URL Handler. Such manipulation of the argument streamIp leads to server-side request forgery. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-5840	A security flaw has been discovered in PHPGurukul News Portal Project 4.1. Impacted is an unknown function of the file /admin/check_availability.php. Performing a manipulation of the argument Username results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-34857	UAF vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	4.7	More Details
CVE-2026-33193	Docmost is open-source collaborative wiki and documentation software. Versions prior to 0.70.0 are vulnerable to a stored cross-site scripting (XSS) attack due to improper handling of MIME type spoofing (GHSL-2026-052). An attacker could exploit this flaw to inject malicious scripts, potentially compromising the security of users and data. Version 0.70.0 contains a patch.	4.6	More Details
CVE-2026-39417	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain an incomplete fix for CVE-2025-53928, where a Remote Code Execution vulnerability still exists in the MCP node of the workflow engine. MaxKB only restricts the referencing code path (loading MCP config from the database). The else branch, responsible for loading mcp_servers directly from user-supplied JSON remains completely unpatched. Since mcp_source is an optional field (required=False), an attacker can simply omit it or set it to any non-referencing value to bypass the fix. By calling the workflow creation API directly with a crafted JSON payload, an attacker can inject a complete MCP node configuration with stdio transport, arbitrary command, and args — achieving RCE when the workflow is triggered via chat. This issue has been fixed in version 2.8.0.	4.6	More Details
CVE-	EspoCRM is an open source customer relationship management application. Versions 9.3.3 and below have a stored HTML injection vulnerability that allows any authenticated user with standard (non-administrative) privileges to inject arbitrary HTML into system-generated email notifications by crafting malicious content in the post field of stream activity notes. The vulnerability exists because server-side Handlebars templates render the post field using unescaped triple-brace syntax, the Markdown processor preserves inline HTML by default, and the rendering pipeline		

2026-33657	explicitly skips sanitization for fields present in additionalData, creating a path where attacker-controlled HTML is accepted, stored, and rendered directly into emails without any escaping. Since the emails are sent using the system's configured SMTP identity (such as an administrative sender address), the injected content appears fully trusted to recipients, enabling phishing attacks, user tracking via embedded resources like image beacons, and UI manipulation within email content. The @mention feature further increases the impact by allowing targeted delivery of malicious emails to specific users. This issue has been fixed in version 9.3.4.	4.6	More Details
CVE-2026-20928	Improper removal of sensitive information before storage or transfer in Windows Recovery Environment Agent allows an unauthorized attacker to bypass a security feature with a physical attack.	4.6	More Details
CVE-2026-22154	An improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to perform a stored cross site scripting (XSS) attack via crafted HTTP Requests.	4.6	More Details
CVE-2026-35659	OpenClaw before 2026.3.22 contains a service discovery vulnerability where TXT metadata from Bonjour and DNS-SD could influence CLI routing even when actual service resolution failed. Attackers can exploit unresolved hints to steer routing decisions to unintended targets by providing malicious discovery metadata.	4.6	More Details
CVE-2026-20945	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	4.6	More Details
CVE-2026-26175	Use of uninitialized resource in Windows Boot Manager allows an unauthorized attacker to bypass a security feature with a physical attack.	4.6	More Details
CVE-2026-2838	The Whole Enquiry Cart for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘woowhole_success_msg’ parameter in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-40025	The Sleuth Kit through 4.14.0 contains an out-of-bounds read vulnerability in the APFS filesystem keybag parser where the wrapped_key_parser class follows attacker-controlled length fields without bounds checking, causing heap reads past the allocated buffer. An attacker can craft a malicious APFS disk image that triggers information disclosure or crashes when processed by any Sleuth Kit tool that parses APFS volumes.	4.4	More Details
CVE-2026-40026	The Sleuth Kit through 4.14.0 contains an out-of-bounds read vulnerability in the ISO9660 filesystem parser where the parse_susp() function trusts len_id, len_des, and len_src fields from the disk image to memcpy data into a stack buffer without verifying that the source data falls within the parsed SUSP block. An attacker can craft a malicious ISO image that causes reads past the end of the SUSP data buffer, and a zero-length SUSP entry can trigger an infinite parsing loop.	4.4	More Details
CVE-2026-32220	Improper access control in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to bypass a security feature locally.	4.4	More Details
CVE-2026-5169	The Inquiry Form to Posts or Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Form Header' field in versions up to and including 1.0. This is due to insufficient input sanitization when saving via update_option() and lack of output escaping when displaying the stored value. The vulnerability exists in two locations: (1) the plugin settings page at inq_form.php line 180 where the value is echoed into an HTML attribute without esc_attr(), and (2) the front-end shortcode output at inquery_form_to_posts_or_pages.php line 139 where the value is output in HTML content without esc_html(). This makes it possible for authenticated attackers with administrator-level access to inject arbitrary web scripts that will execute whenever a user accesses the plugin settings page or views a page containing the [inquiry_form] shortcode.	4.4	More Details
CVE-2026-39864	Kamailio is an open source implementation of a SIP Signaling Server. Prior to 6.0.5 and 5.8.7, an out-of-bounds read in the auth module of Kamailio (formerly OpenSER and SER) allows remote attackers to cause a denial of service (process crash) via a specially crafted SIP packet if a successful user authentication without a database backend is followed by additional user identity checks. This vulnerability is fixed in 6.0.5 and 5.8.7.	4.4	More Details
CVE-2026-24511	Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.1.6 and versions 9.11.0.0 through 9.13.0.0, contains a generation of error message containing sensitive information vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure.	4.4	More Details
CVE-2026-3574	The Experto Dashboard for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's settings fields (including 'Navigation Font Size', 'Navigation Font Weight', 'Heading Font Size', 'Heading Font Weight', 'Text Font Size', and 'Text Font Weight') in all versions up to and including 1.0.4. This is due to insufficient input sanitization (no sanitize callback in register_setting()) and missing output escaping (no esc_attr() in the field_callback() printf output) on user-supplied values. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in the plugin settings page that will execute whenever a user accesses the settings page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details

CVE-2026-4479	The WholeSale Products Dynamic Pricing Management WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-27906	Improper input validation in Windows Hello allows an authorized attacker to bypass a security feature locally.	4.4	More Details
CVE-2026-5869	Heap buffer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-6032	A vulnerability was found in code-projects Simple Laundry System 1.0. This impacts an unknown function of the file /checkcheckout.php. Performing a manipulation of the argument serviceId results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2025-9484	GitLab has remediated an issue in GitLab EE affecting all versions from 16.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that under certain circumstances could have allowed an authenticated user to have access to other users' email addresses via certain GraphQL queries.	4.3	More Details
CVE-2026-5889	Cryptographic Flaw in PDFium in Google Chrome prior to 147.0.7727.55 allowed an attacker to read potentially sensitive information from encrypted PDFs via a brute-force attack. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-27672	The Material Master application does not enforce authorization checks for authenticated users when executing reports, resulting in the disclosure of sensitive information. This vulnerability has a low impact on confidentiality and does not affect integrity and availability of the system.	4.3	More Details
CVE-2026-5891	Insufficient policy enforcement in browser UI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-5906	Incorrect security UI in Omnibox in Google Chrome on Android prior to 147.0.7727.55 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-6034	A flaw has been found in code-projects Vehicle Showroom Management System 1.0. Impacted is an unknown function of the file /BranchManagement/ProfitAndLossReport.php. Executing a manipulation of the argument BRANCH_ID can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2026-27676	Due to missing authorization checks in the SAP S/4HANA OData Service (Manage Technical Object Structures), an attacker could update and delete child entities via exposed OData services without proper authorization. This vulnerability results in a low impact on integrity, while confidentiality and availability are not impacted.	4.3	More Details
CVE-2026-5894	Inappropriate implementation in PDF in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-6035	A vulnerability has been found in code-projects Vehicle Showroom Management System 1.0. The affected element is an unknown function of the file /BranchManagement/ServiceAndSalesReport.php. The manipulation of the argument BRANCH_ID 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-2026-39415	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to 2.46.0, a vulnerability has been identified in Frappe Learning where quiz scores can be modified by students before submission. The application currently relies on client-side calculated scores, which can be altered using browser developer tools prior to sending the submission request. While this does not allow modification of other users' data or privilege escalation, it compromises the integrity of quiz results and undermines academic reliability. This issue affects data integrity but does not expose confidential information or allow unauthorized access to other accounts. This vulnerability is fixed in 2.46.0.	4.3	More Details
CVE-2026-5897	Incorrect security UI in Downloads in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-5898	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-5900	Policy bypass in Downloads in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass of multi-download protections via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache PDFBox Examples. This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.36, from		

CVE-2026-33929	3.0.0 through 3.0.7. Users are recommended to update to version 2.0.37 or 3.0.8 once available. Until then, they should apply the fix provided in GitHub PR 427. The ExtractEmbeddedFiles example contained a path traversal vulnerability (CWE-22) mentioned in CVE-2026-23907. However the change in the releases 2.0.36 and 3.0.7 is flawed because it doesn't consider the file path separator. Because of that, a user having writing rights on /home/ABC could be victim to a malicious PDF resulting in a write attempt to any path starting with /home/ABC, e.g. "/home/ABCDEF". Users who have copied this example into their production code should apply the mentioned change. The example has been changed accordingly and is available in the project repository.	4.3	More Details
CVE-2026-39469	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Softaculous PageLayer pagelayer allows Retrieve Embedded Sensitive Data.This issue affects PageLayer: from n/a through <= 2.0.8.	4.3	More Details
CVE-2026-5887	Insufficient validation of untrusted input in Downloads in Google Chrome on Windows prior to 147.0.7727.55 allowed a remote attacker to bypass download restrictions via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-6000	A vulnerability was found in code-projects Online Library Management System 1.0. Affected is an unknown function of the file /sql/library.sql of the component SQL Database Backup File Handler. Performing a manipulation results in information disclosure. The attack may be initiated remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2026-32202	Protection mechanism failure in Windows Shell allows an unauthorized attacker to perform spoofing over a network.	4.3	More Details
CVE-2026-4977	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WordPress is vulnerable to Improper Access Control in all versions up to, and including, 1.2.58 This is due to insufficient field-level permission validation in the upload_file_remove() AJAX handler where the $htmlvar parameter is not validated against a whitelist of allowed fields or checked against the field's for_admin_use property. This makes it possible for authenticated attackers, with subscriber-level access and above, to clear or reset any restricted usermeta column for their own user record, including fields marked as "For admin use only", bypassing intended field-level access restrictions.	4.3	More Details
CVE-2026-5864	Heap buffer overflow in WebAudio in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-5911	Policy bypass in ServiceWorkers in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-5875	Policy bypass in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-5808	A vulnerability was detected in openstatusHQ openstatus up to 1b678e71a85961ae319cbb214a8eae634059330c. This impacts an unknown function of the file apps/dashboard/src/app/(dashboard)/onboarding/client.tsx of the component Onboarding Endpoint. The manipulation of the argument callbackURL results in cross site scripting. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The patch is identified as 43d9b2b9ef8ae1a98f9bdc8a9f86d6a3dfaa2dfb. It is advisable to implement a patch to correct this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	4.3	More Details
CVE-2026-4330	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to authorization bypass through user-controlled key in all versions up to, and including, 8.8.3. This is due to the plugin's AJAX handlers failing to validate that the user-supplied 'b2s_id' parameter belongs to the current user before performing UPDATE and DELETE operations. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify, reschedule, or delete other users' scheduled social media posts.	4.3	More Details
CVE-2026-5918	Inappropriate implementation in Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2026-1924	The Aruba HiSpeed Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.4. This is due to missing nonce verification on the `ahsc_ajax_reset_options()` function. This makes it possible for unauthenticated attackers to reset all plugin settings to their default values via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-34225	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Versions 0.7.2 and below contain a Blind Server Side Request Forgery in the functionality that allows editing an image via a prompt. The affected function performs a GET request to a user-provided URL with no restriction on the domain, allowing the local address space to be accessed. Since the SSRF is blind (the response cannot be read), the primary impact is port scanning of the local network, as whether a port is open can be determined based on whether the GET request succeeds or fails. These response differentials can be automated to iterate through the entire port range and identify open ports. If the service running on an open port can be inferred, an attacker may be able to interact with it in a meaningful way, provided the service offers state-changing GET request endpoints. This issue was unresolved at the time of publication.	4.3	More Details

CVE-2026-33829	Exposure of sensitive information to an unauthorized actor in Windows Snipping Tool allows an unauthorized attacker to perform spoofing over a network.	4.3	More Details
CVE-2026-4141	The Quran Translations plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.7. This is due to missing nonce validation in the quran_playlist_options() function that handles the plugin's settings page. The function processes POST requests to update plugin options via update_option() without any wp_nonce_field() in the form or wp_verify_nonce()/check_admin_referer() verification before processing. This makes it possible for unauthenticated attackers to modify plugin settings (toggling display options for PDF, RSS, podcast, media player links, playlist title, and playlist code) via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-70811	Cross Site Request Forgery vulnerability in Phpbb phbb3 v.3.3.15 allows a local attacker to execute arbitrary code via the Admin Control Panel icon management functionality.	4.3	More Details
CVE-2025-59809	A server-side request forgery (ssrf) vulnerability [CWE-918] vulnerability in Fortinet FortiSOAR PaaS 7.6.4, FortiSOAR PaaS 7.6.0 through 7.6.2, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.4, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated attacker to discover services running on local ports via crafted requests.	4.3	More Details
CVE-2026-4057	The Download Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `makeMediaPublic()` and `makeMediaPrivate()` functions in all versions up to, and including, 3.3.51. This is due to the functions only checking for `edit_posts` capability without verifying post ownership via `current_user_can('edit_post', $id)`, and the destructive operations executing before the admin-level check in `mediaAccessControl()`. This makes it possible for authenticated attackers, with Contributor-level access and above, to strip all protection metadata (password, access restrictions, private flag) from any media file they do not own, making admin-protected files publicly accessible via their direct URL.	4.3	More Details
CVE-2026-5878	Incorrect security UI in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-5880	Insufficient policy enforcement in browser UI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-5882	Incorrect security UI in Fullscreen in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2026-35642	OpenClaw before 2026.3.25 contains an authorization bypass vulnerability where group reaction events bypass the requireMention access control mechanism. Attackers can trigger reactions in mention-gated groups to enqueue agent-visible system events that should remain restricted.	4.3	More Details
CVE-2026-5867	Heap buffer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-35598	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the CalDAV GetResource and GetResourcesByList methods fetch tasks by UID from the database without verifying that the authenticated user has access to the task's project. Any authenticated CalDAV user who knows (or guesses) a task UID can read the full task data from any project on the instance. This vulnerability is fixed in 2.3.0.	4.3	More Details
CVE-2026-39476	Missing Authorization vulnerability in Syed Balkhi User Feedback userfeedback-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Feedback: from n/a through <= 1.10.1.	4.3	More Details
CVE-2026-39592	Missing Authorization vulnerability in Andy Ha DEPART depart-deposit-and-part-payment-for-woo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects DEPART: from n/a through <= 1.0.7.	4.3	More Details
CVE-2026-5825	A vulnerability was detected in code-projects Simple Laundry System 1.0. This vulnerability affects unknown code of the file /delmemberinfo.php. Performing a manipulation of the argument userid results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-39565	Missing Authorization vulnerability in magepeopleteam WpTravelly tour-booking-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WpTravelly: from n/a through <= 2.1.7.	4.3	More Details
CVE-2026-40041	Pachno 1.0.6 contains a cross-site request forgery vulnerability that allows attackers to perform arbitrary actions in authenticated user context by exploiting missing CSRF protections on state-changing endpoints. Attackers can craft malicious requests targeting login, registration, file upload, milestone editing, and administrative functions to force logout, create accounts, modify roles, inject comments, or upload files when authenticated users visit attacker-controlled websites.	4.3	More Details

CVE-2026-5826	A flaw has been found in code-projects Simple IT Discussion Forum 1.0. This issue affects some unknown processing of the file /edit-category.php. Executing a manipulation of the argument Category can lead to cross site scripting. The attack can be launched remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2026-3568	The MStore API plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.18.3. This is due to the update_user_profile() function in controllers/flutter-user.php processing the 'meta_data' JSON parameter without any allowlist, blocklist, or validation of meta keys. The function reads raw JSON from php://input (line 1012), decodes it (line 1013), authenticates the user via cookie validation (line 1015), and then directly iterates over the user-supplied meta_data array passing arbitrary keys and values to update_user_meta() (line 1080) with no sanitization or restrictions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify arbitrary user meta fields on their own accounts, including sensitive fields like wp_user_level (to escalate to administrator-level legacy checks), plugin-specific authorization flags (e.g., _wpuf_user_active, aiowps_account_status), and billing/profile fields with unsanitized values (potentially enabling Stored XSS in admin contexts). Note that wp_capabilities cannot be directly exploited this way because it requires a serialized array value, but wp_user_level (a simple integer) and numerous plugin-specific meta keys are exploitable.	4.3	More Details
CVE-2026-3371	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.9.7. This is due to missing authorization checks in the `save_course_content_order()` private method, which is called unconditionally by the `tutor_update_course_content_order` AJAX handler. While the handler's `content_parent` branch includes a `can_user_manage()` check, the `save_course_content_order()` call processes attacker-supplied `tutor_topics_lessons_sorting` JSON without any ownership or capability verification. This makes it possible for authenticated attackers with Subscriber-level access or above to detach lessons from topics, reorder course content, and reassign lessons between topics in any course, including admin-owned courses, by sending a crafted AJAX request with manipulated topic and lesson IDs.	4.3	More Details
CVE-2026-33460	Incorrect Authorization (CWE-863) in Kibana can lead to cross-space information disclosure via Privilege Abuse (CAPEC-122). A user with Fleet agent management privileges in one Kibana space can retrieve Fleet Server policy details from other spaces through an internal enrollment endpoint. The endpoint bypasses space-scoped access controls by using an unscoped internal client, returning operational identifiers, policy names, management state, and infrastructure linkage details from spaces the user is not authorized to access.	4.3	More Details
CVE-2026-6109	A vulnerability was determined in FoundationAgents MetaGPT up to 0.8.1. The impacted element is the function evaluateCode of the file metagpt/environment/minecraft/mineflayer/index.js of the component Mineflayer HTTP API. Executing a manipulation can lead to cross-site request forgery. The attack may be performed from remote. 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-2026-35023	Wimi Teamwork On-Premises versions prior to 8.2.0 contain an insecure direct object reference vulnerability in the preview.php endpoint where the item_id parameter lacks proper authorization checks. Attackers can enumerate sequential item_id values to access and retrieve image previews from other users' private or group conversations, resulting in unauthorized disclosure of sensitive information.	4.3	More Details
CVE-2019-25708	Heatmiser Wifi Thermostat 1.7 contains a cross-site request forgery vulnerability that allows attackers to change administrator credentials by tricking authenticated users into submitting malicious requests. Attackers can craft HTML forms targeting the networkSetup.htm endpoint with parameters usnm, usps, and cfps to modify the admin username and password without user consent.	4.3	More Details
CVE-2026-33146	Docmost is open-source collaborative wiki and documentation software. An authorization bypass vulnerability in versions 0.70.0 through 0.70.2 exposes restricted child page titles and text snippets through the public search endpoint (`POST /api/search/share-search`) for publicly shared content. This flaw allows unauthenticated users to enumerate and retrieve content that should remain hidden from public share viewers, leading to a confidentiality breach. Version 0.70.3 contains a patch.	4.3	More Details
CVE-2026-6231	The bson_validate function may return early on specific inputs and incorrectly report success. This behavior could result in skipping validation for BSON data, allowing malformed or invalid UTF-8 sequences to bypass validation and be processed incorrectly. The issue may affect applications that rely on these functions to validate untrusted BSON data before further processing. This issue affects MongoDB C Driver versions prior to 1.30.5, MongoDB C Driver version 2.0.0 and MongoDB C Driver version 2.0.1	4.3	More Details
CVE-2026-6150	A vulnerability has been found in code-projects Simple Laundry System 1.0. This affects an unknown part of the file /checkupdatestatus.php. The manipulation of the argument serviceId leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-1673	The BEAR – Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.5. This is due to missing nonce validation on the woobe_delete_tax_term() function. This makes it possible for unauthenticated attackers to delete WooCommerce taxonomy terms (categories, tags, etc.) via a forged request granted they can trick a site administrator or shop manager into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-5960	A weakness has been identified in code-projects Patient Record Management System 1.0. This affects an unknown part of the file /db/hcpms.sql of the component SQL Database Backup File Handler. Executing a manipulation can lead to information disclosure. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-	A vulnerability has been found in code-projects Simple ChatBox up to 1.0. Affected by this vulnerability is an unknown		

2026-6159	functionality of the file /chatbox/insert.php of the component Endpoint. Such manipulation of the argument msg leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-39618	Cross-Site Request Forgery (CSRF) vulnerability in themearile NewsExo newsexo allows Cross Site Request Forgery.This issue affects NewsExo: from n/a through <= 7.1.	4.3	More Details
CVE-2026-5847	A vulnerability has been found in code-projects Movie Ticketing System 1.0. Impacted is an unknown function of the file /db/moviedb.sql of the component SQL Database Backup File Handler. Such manipulation leads to information disclosure. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-39627	Missing Authorization vulnerability in wproyal Ashe ashe allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ashe: from n/a through <= 2.266.	4.3	More Details
CVE-2026-33005	Improper Handling of Insufficient Privileges vulnerability in Apache OpenMeetings. Any registered user can query web service with their credentials and get files/sub-folders of any folder by ID (metadata only NOT contents). Metadata includes id, type, name and some other field. Full list of fields get be checked at FileItemDTO object. This issue affects Apache OpenMeetings: from 3.10 before 9.0.0. Users are recommended to upgrade to version 9.0.0, which fixes the issue.	4.3	More Details
CVE-2026-33118	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2026-39985	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. Prior to 27.0.3 and 28.0.1, the redirect parameter upon login to LORIS was not validating the value of the redirect as being within LORIS, which could be used to trick users into visiting arbitrary URLs if they are given a link with a third party redirect parameter. This vulnerability is fixed in 27.0.3 and 28.0.1.	4.3	More Details
CVE-2026-39653	Missing Authorization vulnerability in Deepen Bajracharya Video Conferencing with Zoom video-conferencing-with-zoom-api allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Video Conferencing with Zoom: from n/a through <= 4.6.6.	4.3	More Details
CVE-2026-35662	OpenClaw before 2026.3.22 fails to enforce controlScope restrictions on the send action, allowing leaf subagents to message controlled child sessions beyond their authorized scope. Attackers can exploit this by using the send action to communicate with child sessions without proper scope validation, bypassing intended access control restrictions.	4.3	More Details
CVE-2026-39477	Missing Authorization vulnerability in Brainstorm Force CartFlows cartflows allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CartFlows: from n/a through <= 2.2.3.	4.3	More Details
CVE-2026-1752	GitLab has remediated an issue in GitLab EE affecting all versions from 11.3 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user with developer-role permissions to modify protected environment settings due to improper authorization checks in the API.	4.3	More Details
CVE-2026-39485	Missing Authorization vulnerability in embedplus Youtube Embed Plus youtube-embed-plus allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Youtube Embed Plus: from n/a through <= 14.2.4.	4.3	More Details
CVE-2026-2104	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user to access confidential issues assigned to other users via CSV export due to insufficient authorization checks.	4.3	More Details
CVE-2026-35596	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the hasAccessToLabel function contains a SQL operator precedence bug that allows any authenticated user to read any label that has at least one task association, regardless of project access. Label titles, descriptions, colors, and creator information are exposed. This vulnerability is fixed in 2.3.0.	4.3	More Details
CVE-2026-6218	A vulnerability was found in aandrew-me ytDownloader up to 3.20.2. Affected by this issue is the function createTextNode of the component Error Details Panel. The manipulation results in cross site scripting. The attack may be performed from remote. The vendor was contacted early about this disclosure.	4.3	More Details
CVE-2026-35619	OpenClaw before 2026.3.24 contains an authorization bypass vulnerability in the HTTP /v1/models endpoint that fails to enforce operator read scope requirements. Attackers with only operator.approvals scope can enumerate gateway model metadata through the HTTP compatibility route, bypassing the stricter WebSocket RPC authorization checks.	4.3	More Details
CVE-2026-22576	A storing passwords in a recoverable format vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.4, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.4, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to retrieve passwords for multiple installed connectors via server address modification in connector configuration.	4.3	More Details
CVE-2026-2619	GitLab has remediated an issue in GitLab EE affecting all versions from 18.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that under certain circumstances could have allowed an authenticated user with auditor privileges to modify vulnerability flag data in private projects due to incorrect authorization.	4.3	More Details

CVE-2026-35651	OpenClaw versions 2026.2.13 through 2026.3.24 contain an ANSI escape sequence injection vulnerability in approval prompts that allows attackers to spoof terminal output. Untrusted tool metadata can carry ANSI control sequences into approval prompts and permission logs, enabling attackers to manipulate displayed information through malicious tool titles.	4.3	More Details
CVE-2026-4109	The Eventin – Events Calendar, Event Booking, Ticket & Registration (AI Powered) plugin for WordPress is vulnerable to unauthorized access of data due to a improper capability check on the get_item_permissions_check() function in all versions up to, and including, 4.1.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary order data including customer PII (name, email, phone) by iterating order IDs.	4.3	More Details
CVE-2026-39506	Missing Authorization vulnerability in Jordy Meow AI Engine (Pro) ai-engine-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI Engine (Pro): from n/a through < 3.4.2.	4.3	More Details
CVE-2026-0814	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'vsz_cf7_export_to_excel' function in all versions up to, and including, 2.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export form submissions to excel file.	4.3	More Details
CVE-2026-33534	EspoCRM is an open source customer relationship management application. Versions 9.3.3 and below have an authenticated Server-Side Request Forgery (SSRF) vulnerability that allows bypassing the internal-host validation logic by using alternative IPv4 representations such as octal notation (e.g., 0177.0.0.1 instead of 127.0.0.1). This is caused by HostCheck::isNotInternalHost() function relying on PHP's filter_var(..., FILTER_VALIDATE_IP), which does not recognize alternative IP formats, causing the validation to fall through to a DNS lookup that returns no records and incorrectly treats the host as safe, however the cURL subsequently normalizes the address and connects to the loopback destination. Through the confirmed /api/v1/Attachment/fromImageUrl endpoint, an authenticated user can force the server to make requests to loopback-only services and store the fetched response as an attachment. This vulnerability is distinct from CVE-2023-46736 (which involved redirect-based SSRF) and may allow access to internal resources reachable from the application runtime. This issue has been fixed in version 9.3.4.	4.3	More Details
CVE-2026-34719	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, the webhook model was missing a proper validation for loop back addresses, or link-local addresses — only the URL scheme (HTTP/HTTPS) as well as the hostname was checked. This could end up in retrieving confidential metadata of cloud/hosting providers. The existing check is now extended and is applied when configuring webhooks as well as triggering webhook jobs. This vulnerability is fixed in 7.0.1 and 6.5.4.	4.3	More Details
CVE-2026-40103	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, Vikunja's scoped API token enforcement for custom project background routes is method-confused. A token with only projects.background can successfully delete a project background, while a token with only projects.background_delete is rejected. This is a scoped-token authorization bypass. This vulnerability is fixed in 2.3.0.	4.3	More Details
CVE-2026-35041	fast-jwt provides fast JSON Web Token (JWT) implementation. From 5.0.0 to 6.2.0, a denial-of-service condition exists in fast-jwt when the allowedAud verification option is configured using a regular expression. Because the aud claim is attacker-controlled and the library evaluates it against the supplied RegExp, a crafted JWT can trigger catastrophic backtracking in the JavaScript regex engine, resulting in significant CPU consumption during verification. This vulnerability is fixed in 6.2.1.	4.2	More Details
CVE-2026-24318	Due to an Insecure session management vulnerability in SAP Business Objects Business Intelligence Platform, an unauthenticated attacker could obtain valid session tokens and reuse them to gain unauthorized access to a victim's session. If the application continues to accept previously issued tokens after authentication, the attacker could assume the victim's authenticated context. This could allow the attacker to access or modify information within the victim's session scope, impacting confidentiality and integrity, while availability remains unaffected.	4.2	More Details
CVE-2026-39413	LightRAG provides simple and fast retrieval-augmented generation. Prior to 1.4.14, the LightRAG API is vulnerable to a JWT algorithm confusion attack where an attacker can forge tokens by specifying 'alg': 'none' in the JWT header. Since the jwt.decode() call does not explicitly deny the 'none' algorithm, a crafted token without a signature will be accepted as valid, leading to unauthorized access. This vulnerability is fixed in 1.4.14.	4.2	More Details
CVE-2026-35617	OpenClaw before 2026.3.25 contains an authorization bypass vulnerability in Google Chat group policy enforcement that relies on mutable space display names. Attackers can rebind group policies by changing or colliding space display names to gain unauthorized access to protected resources.	4.2	More Details
CVE-2026-35624	OpenClaw before 2026.3.22 contains a policy confusion vulnerability in room authorization that matches colliding room names instead of stable room tokens. Attackers can exploit similarly named rooms to bypass allowlist policies and gain unauthorized access to protected Nextcloud Talk rooms.	4.2	More Details
CVE-2026-34858	UAF vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	4.1	More Details
CVE-2026-27683	SAP BusinessObjects Business Intelligence application allows an authenticated attacker to inject malicious JavaScript payloads through crafted URLs. When a victim accesses the URL, the script executes in the user's browser, potentially exposing restricted information. This results in a low impact on confidentiality with no impact on integrity and availability.	4.1	More Details
CVE-	A storing passwords in a recoverable format vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.4, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise		More

2026-22574	7.6.0 through 7.6.4, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to retrieve Service account password via server address modification in LDAP configuration.	4.1	Details
CVE-2026-34860	Access control vulnerability in the memo module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	4.1	More Details
CVE-2026-35601	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the CalDAV output generator builds iCalendar VTODO entries via raw string concatenation without applying RFC 5545 TEXT value escaping. User-controlled task titles containing CRLF characters break the iCalendar property boundary, allowing injection of arbitrary iCalendar properties such as ATTACH, VALARM, or ORGANIZER. This vulnerability is fixed in 2.3.0.	4.1	More Details
CVE-2026-39572	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in magepeopleteam Bus Ticket Booking with Seat Reservation bus-ticket-booking-with-seat-reservation allows Retrieve Embedded Sensitive Data.This issue affects Bus Ticket Booking with Seat Reservation: from n/a through < 5.6.5.	4.0	More Details
CVE-2026-40396	Varnish Cache 9 before 9.0.1 allows a "workspace overflow" denial of service (daemon panic) after timeout_linger. A malicious client could send an HTTP/1 request, wait long enough until the session releases its worker thread (timeout_linger) and resume traffic before the session is closed (timeout_idle) sending more than one request at once to trigger a pipelining operation between requests. This vulnerability affecting Varnish Cache 9.0.0 emerged from a port of the Varnish Enterprise non-blocking architecture for HTTP/2. New code was needed to adapt to a more recent workspace API that formalizes the pipelining operation. In addition to the workspace change on the Varnish Cache side, other differences created merge conflicts, like partial support for trailers in Varnish Enterprise. The conflict resolution missed one code path configuring pipelining to perform a complete workspace rollback, losing the guarantee that prefetched data would fit inside workspace_client during the transition from one request to the next. This can result in a workspace overflow, triggering a panic and crashing the Varnish server.	4.0	More Details
CVE-2026-39566	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Designinvento DirectoryPress directorypress allows Retrieve Embedded Sensitive Data.This issue affects DirectoryPress: from n/a through <= 3.6.26.	4.0	More Details
CVE-2026-33555	An issue was discovered in HAProxy before 3.3.6. The HTTP/3 parser does not check that the received body length matches a previously announced content-length when the stream is closed via a frame with an empty payload. This can cause desynchronization issues with the backend server and could be used for request smuggling. The earliest affected version is 2.6.	4.0	More Details
CVE-2026-40394	Varnish Cache 9 before 9.0.1 and Varnish Enterprise before 6.0.16r11 allows a "workspace overflow" denial of service (daemon panic) for certain amounts of prefetched data. The setup of an HTTP/2 session starts with a speculative HTTP/1 transport, and upon upgrading to h2 the HTTP/1 request is repurposed as stream zero. During the upgrade, a buffer allocation is made to reserve space to send frames to the client. This allocation would split the original workspace, and depending on the amount of prefetched data, the next fetch could perform a pipelining operation that would run out of workspace.	4.0	More Details
CVE-2026-40386	In libexif through 0.6.25, an integer underflow in size checking for Fuji and Olympus MakerNote decoding could be used by attackers to crash or leak information out of libexif-using programs.	4.0	More Details
CVE-2026-40385	In libexif through 0.6.25, an unsigned 32bit integer overflow in Nikon MakerNote handling could be used by local attackers to cause crashes or information leaks. This only affects 32bit systems.	4.0	More Details
CVE-2026-40395	Varnish Enterprise before 6.0.16r12 allows a "workspace overflow" denial of service (daemon panic) for shared VCL. The headerplus.write_req0() function from vmod_headerplus updates the underlying req0, which is normally the original read-only request from which req is derived (readable and writable from VCL). This is useful in the active VCL, after amending req, to prepare a refined req0 before switching to a different VCL with the return (vcl(<label>)) action. This is for example how the Varnish Controller operates shared VCL deployments. If the amended req contained too many header fields for req0, this would have resulted in a workspace overflow that would in turn trigger a panic and crash the Varnish Enterprise server. This could be used as a Denial of Service attack vector by malicious clients.	4.0	More Details
CVE-2026-24661	Mattermost Plugins versions <=2.1.3.0 fail to limit the request body size on the {{/changes}} webhook endpoint which allows an authenticated attacker to cause memory exhaustion and denial of service via sending an oversized JSON payload. Mattermost Advisory ID: MMSA-2026-00611	3.7	More Details
CVE-2026-34166	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.25.3, the replace filter in LiquidJS incorrectly accounts for memory usage when the memoryLimit option is enabled. It charges str.length + pattern.length + replacement.length bytes to the memory limiter, but the actual output from str.split(pattern).join(replacement) can be quadratically larger when the pattern occurs many times in the input string. This allows an attacker who controls template content to bypass the memoryLimit DoS protection with approximately 2,500x amplification, potentially causing out-of-memory conditions. This vulnerability is fixed in 10.25.3.	3.7	More Details
CVE-2026-21388	Mattermost Plugins versions <=2.3.1 fail to limit the request body size on the {{/lifecycle}} webhook endpoint which allows an authenticated attacker to cause memory exhaustion and denial of service via sending an oversized JSON payload. Mattermost Advisory ID: MMSA-2026-00610	3.7	More Details

CVE-2026-40097	Step CA is an online certificate authority for secure, automated certificate management for DevOps. From 0.24.0 to before 0.30.0-rc3, an attacker can trigger an index out-of-bounds panic in Step CA by sending a crafted attestation key (AK) certificate with an empty Extended Key Usage (EKU) extension during TPM device attestation. When processing a device-attest-01 ACME challenge using TPM attestation, Step CA validates that the AK certificate contains the tcg-kp-AIKCertificate Extended Key Usage OID. During this validation, the EKU extension value is decoded from its ASN.1 representation and the first element is checked. A crafted certificate could include an EKU extension that decodes to an empty sequence, causing the code to panic when accessing the first element of the empty slice. This vulnerability is only reachable when a device-attest-01 ACME challenge with TPM attestation is configured. Deployments not using TPM device attestation are not affected. This vulnerability is fixed in 0.30.0-rc3.	3.7	More Details
CVE-2026-40184	TREK is a collaborative travel planner. Prior to 2.7.2, TREK served uploaded photos without requiring authentication. This vulnerability is fixed in 2.7.2.	3.7	More Details
CVE-2026-40194	phpseclib is a PHP secure communications library. Prior to 3.0.51, 2.0.53, and 1.0.28, phpseclib\Net\SSH2::get_binary_packet() uses PHP's != operator to compare a received SSH packet HMAC against the locally computed HMAC. != on equal-length binary strings in PHP uses memcmp(), which short-circuits on the first differing byte. This is a real variable-time comparison (CWE-208), proven by scaling benchmarks. This vulnerability is fixed in 3.0.51, 2.0.53, and 1.0.28.	3.7	More Details
CVE-2026-35648	OpenClaw before 2026.3.22 contains a policy bypass vulnerability where queued node actions are not revalidated against current command policy when delivered. Attackers can exploit stale allowlists or declarations that survive policy tightening to execute unauthorized commands.	3.7	More Details
CVE-2025-40745	A vulnerability has been identified in Siemens Software Center (All versions < V3.5.8.2), Simcenter 3D (All versions < V2506.6000), Simcenter Femap (All versions < V2506.0002), Simcenter STAR-CCM+ (All versions < V2602), Solid Edge SE2025 (All versions < V225.0 Update 13), Solid Edge SE2026 (All versions < V226.0 Update 04), Tecnomatix Plant Simulation (All versions < V2504.0008). Affected applications do not properly validate client certificates to connect to Analytics Service endpoint. This could allow an unauthenticated remote attacker to perform man in the middle attacks.	3.7	More Details
CVE-2026-6107	A flaw has been found in 1Panel-dev MaxKB up to 2.6.1. This issue affects some unknown processing of the file apps/common/middleware/chat_headers_middleware.py of the component ChatHeadersMiddleware. This manipulation of the argument Name causes cross site scripting. Remote exploitation of the attack is possible. Upgrading to version 2.8.0 is capable of addressing this issue. Patch name: 026a2d623e2aa5efa67c4834651e79d5d7cab1da. 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.	3.5	More Details
CVE-2026-5810	A flaw has been found in SourceCodester Sales and Inventory System 1.0. Affected is an unknown function of the file /delete.php of the component GET Parameter Handler. This manipulation of the argument ID causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used.	3.5	More Details
CVE-2026-40077	Beszel is a server monitoring platform. Prior to 0.18.7, some API endpoints in the Beszel hub accept a user-supplied system ID and proceed without further checks that the user should have access to that system. As a result, any authenticated user can access these routes for any system if they know the system's ID. System IDs are random 15 character alphanumeric strings, and are not exposed to all users. However, it is theoretically possible for an authenticated user to enumerate a valid system ID via web API. To use the containers endpoints, the user would also need to enumerate a container ID, which is 12 digit hexadecimal string. This vulnerability is fixed in 0.18.7.	3.5	More Details
CVE-2026-6216	A security vulnerability has been detected in DbGate up to 7.1.4. This affects an unknown function of the file packages/web/src/icons/FontIcon.svelte of the component SVG Icon String Handler. Such manipulation of the argument applicationIcon leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 7.1.5 mitigates this issue. It is advisable to upgrade the affected component.	3.5	More Details
CVE-2026-33659	EspoCRM is an open source customer relationship management application. In versions 9.3.3 and below, the POST /api/v1/Attachment/fromImageUrl endpoint is vulnerable to Server-Side Request Forgery (SSRF) via a DNS rebinding (TOCTOU) condition. Host validation uses dns_get_record() but the actual HTTP request resolves hostnames through curl's internal resolver (gethostbyname()), allowing the two lookups to return different IP addresses for the same hostname. A secondary issue exists where an empty DNS result (due to DNS failure, IPv6-only domains, or non-existent hostnames) causes the validation to implicitly allow the host without further checks. An authenticated attacker with default attachment creation access can exploit this gap to bypass internal IP restrictions and scan internal network ports, confirm the existence of internal hosts, and interact with internal HTTP-based services, though data extraction from binary protocol services and remote code execution are not possible through this endpoint. This issue has been fixed in version 9.3.4.	3.5	More Details
CVE-2026-5806	A security vulnerability has been detected in code-projects Easy Blog Site 1.0. This affects an unknown function of the file /posts/update.php. The manipulation of the argument postTitle leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2025-15632	A vulnerability has been found in 1Panel-dev MaxKB up to 2.4.2. Impacted is an unknown function of the file ui/src/chat.ts of the component MdPreview. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.5.0 is recommended to address this issue. The name of the patch is 7230daa5ec3e6574b6ede83dd48a4fbc0e70b8d8. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professional	3.5	More Details

	manner and quickly released a fixed version of the affected product.		
CVE-2026-33551	An issue was discovered in OpenStack Keystone 14 through 26 before 26.1.1, 27.0.0, 28.0.0, and 29.0.0. Restricted application credentials can create EC2 credentials. By using a restricted application credential to call the EC2 credential creation API, an authenticated user with only a reader role may obtain an EC2/S3 credential that carries the full set of the parent user's S3 permissions, effectively bypassing the role restrictions imposed on the application credential. Only deployments that use restricted application credentials in combination with the EC2/S3 compatibility API (swift3 / s3api) are affected.	3.5	More Details
CVE-2026-6162	A vulnerability has been found in PHPGurukul Company Visitor Management System 2.0. This impacts an unknown function of the file /bwdates-reports-details.php. The manipulation of the argument fromdate leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2026-34454	OAuth2 Proxy is a reverse proxy that provides authentication using OAuth2 providers. A regression introduced in 7.11.0 prevents OAuth2 Proxy from clearing the session cookie when rendering the sign-in page. In deployments that rely on the sign-in page as part of their logout flow, a user may be shown the sign-in page while the existing session cookie remains valid, meaning the browser session is not actually logged out. On shared workstations or devices, a subsequent user could continue to use the previous user's authenticated session. Deployments that use a dedicated logout/sign-out endpoint to terminate sessions are not affected. This issue is fixed in 7.15.2	3.5	More Details
CVE-2026-6106	A vulnerability was detected in 1Panel-dev MaxKB up to 2.2.1. This vulnerability affects the function StaticHeadersMiddleware of the file apps/common/middleware/static_headers_middleware.py of the component Public Chat Interface. The manipulation of the argument Name results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used. Upgrading to version 2.8.0 is able to resolve this issue. The patch is identified as 026a2d623e2aa5efa67c4834651e79d5d7cab1da. It is recommended 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.	3.5	More Details
CVE-2026-35400	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 20.0.0 to before 27.0.3 and 28.0.1, an endpoint in the publication module was incorrectly trusting the baseURL submitted by a user's POST request rather than the internal LORIS value. This could result in a theoretical attacker with publication module access forging an email to an external domain under the attacker's control which appeared to come from LORIS. This vulnerability is fixed in 27.0.3 and 28.0.1.	3.5	More Details
CVE-2026-28264	Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	3.3	More Details
CVE-2026-21012	External control of file name in AODManager prior to SMR Apr-2026 Release 1 allows privileged local attacker to create file with system privilege.	3.3	More Details
CVE-2026-6042	A security flaw has been discovered in musl libc up to 1.2.6. Affected is the function iconv of the file src/locale/iconv.c of the component GB18030 4-byte Decoder. Performing a manipulation results in inefficient algorithmic complexity. The attack must be initiated from a local position. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-6192	A vulnerability was identified in uclouvain openjpeg up to 2.5.4. This impacts the function opj_pi_initialise_encode in the library src/lib/openjp2/pi.c. The manipulation leads to integer overflow. The attack must be carried out locally. The exploit is publicly available and might be used. The identifier of the patch is 839936aa33eb8899bbbd80fda02796bb65068951. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2026-40109	Flux notification-controller is the event forwarder and notification dispatcher for the GitOps Toolkit controllers. Prior to 1.8.3, the gcr Receiver type in Flux notification-controller does not validate the email claim of Google OIDC tokens used for Pub/Sub push authentication. This allows any valid Google-issued token, to authenticate against the Receiver webhook endpoint, triggering unauthorized Flux reconciliations. Exploitation requires the attacker to know the Receiver's webhook URL. The webhook path is generated as /hook/sha256sum(token+name+namespace), where the token is a random string stored in a Kubernetes Secret. There is no API or endpoint that enumerates webhook URLs. An attacker cannot discover the path without either having access to the cluster and permissions to read the Receiver's .status.webhookPath in the target namespace, or obtaining the URL through other means (e.g. leaked secrets or access to Pub/Sub config). Upon successful authentication, the controller triggers a reconciliation for all resources listed in the Receiver's .spec.resources. However, the practical impact is limited: Flux reconciliation is idempotent, so if the desired state in the configured sources (Git, OCI, Helm) has not changed, the reconciliation results in a no-op with no effect on cluster state. Additionally, Flux controllers deduplicate reconciliation requests, sending many requests in a short period results in only a single reconciliation being processed. This vulnerability is fixed in 1.8.3.	3.1	More Details
CVE-2026-39419	MaxKB is an open-source AI assistant for enterprise. In versions 2.7.1 and below, an authenticated user can bypass sandbox result validation and spoof tool execution results by exploiting Python frame introspection to read the wrapper's UUID from its bytecode constants, then writing a forged result directly to file descriptor 1 (bypassing stdout redirection). By calling sys.exit(0), the attacker terminates the wrapper before it prints the legitimate output, causing the MaxKB service to parse and trust the spoofed response as the genuine tool result. This issue has been fixed in version 2.8.0.	3.1	More Details
CVE-			

2026-40354	Flatpak xdg-desktop-portal before 1.20.4 and 1.21.x before 1.21.1 allows any Flatpak app to trash any file in the host context via a symlink attack on g_file_trash.	2.9	More Details
CVE-2026-40228	In systemd 259, systemd-journald can send ANSI escape sequences to the terminals of arbitrary users when a "logger -p emerg" command is executed, if ForwardToWall=yes is set.	2.9	More Details
CVE-2026-36938	Sourcecodester Online Resort Management System v1.0 is vulnerable to SQL injection in /orms/admin/rooms/view_room.php.	2.7	More Details
CVE-2026-36937	Sourcecodester Online Resort Management System v1.0 is vulnerable to SQL injection in /orms/admin/reservations/view_details.php.	2.7	More Details
CVE-2026-36943	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerable to SQL injection in the file /rsms/admin/repairs/manage_repair.php.	2.7	More Details
CVE-2026-36950	Sourcecodester Online Thesis Archiving System v1.0 is vulnerable to SQL injection in /otas/projects_per_department.php.	2.7	More Details
CVE-2026-36952	Sourcecodester Online Thesis Archiving System v1.0 is vulnerable to SQL injection in the file /otas/admin/curriculum/manage_curriculum.php.	2.7	More Details
CVE-2026-36945	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerable to SQL injection in the file /rsms/admin/clients/manage_client.php	2.7	More Details
CVE-2026-36944	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerale to SQL injection in the file/rsms/admin/repairs/view_details.php.	2.7	More Details
CVE-2026-36873	Sourcecodester Basic Library System v1.0 is vulnerable to SQL Injection in /librarysystem/load_admin.php.	2.7	More Details
CVE-2026-36942	Sourcecodester Online Resort Management System v1.0 is vulnerable to SQL injection in the file /orms/admin/activities/manage_activity.php.	2.7	More Details
CVE-2026-36941	Sourcecodester Online Resort Management System v1.0 is vulnerable to SQL Injection in the file /orms/admin/rooms/manage_room.php.	2.7	More Details
CVE-2026-36947	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerable to SQL Injection in the file /rsms/admin/services/view_service.php.	2.7	More Details
CVE-2026-36923	Sourcecodester Cab Management System 1.0 is vulnerable to SQL Injection in the file /cms/admin/bookings/view_booking.php.	2.7	More Details
CVE-2026-36922	Sourcecodester Cab Management System v1.0 is vulnerable to SQL injection in the file /cms/admin/categories/view_category.php.	2.7	More Details
CVE-2026-36920	Sourcecodester Online Reviewer System v1.0 is vulnerable to SQL Injection in the file /system/system/admins/assessments/examproper/questions-view.php.	2.7	More Details
CVE-2026-36919	Sourcecodester Online Reviewer System v1.0 is vulnerale to SQL Injection in the file /system/system/admins/assessments/examproper/exam-update.php.	2.7	More Details
CVE-2026-36874	Sourcecodester Basic Library System v1.0 is vulnerable to SQL Injection in /librarysystem/load_student.php.	2.7	More Details
CVE-2026-27316	A insufficiently protected credentials vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4 all versions, FortiSandbox PaaS 5.0.1 through 5.0.5 may allow an authenticathed administrator to read LDAP server credentials via client-side inspection.	2.7	More Details
CVE-2026-	Sourcecodester Basic Library System v1.0 is vulnerable to SQL Injection in /librarysystem/load_book.php.	2.7	More Details

36872			
CVE-2026-39510	Authorization Bypass Through User-Controlled Key vulnerability in WP Chill Image Photo Gallery Final Tiles Grid final-tiles-grid-gallery-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Photo Gallery Final Tiles Grid: from n/a through <= 3.6.11.	2.7	More Details
CVE-2026-4916	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user with custom role permissions to demote or remove higher-privileged group members due to improper authorization checks on member management operations.	2.7	More Details
CVE-2026-36946	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerable to SQL injection in the file /rsms/admin/inquiries/view_details.php.	2.7	More Details
CVE-2026-37598	SourceCodester Patient Appointment Scheduler System v1.0 is vulnerable to arbitrary code execution (RCE) via /scheduler/classes/SystemSettings.php?f=update_settings.	2.7	More Details
CVE-2026-37595	SourceCodester Online Employees Work From Home Attendance System v1.0 is vulnerable to SQL Injection in the file /wfh_attendance/admin/manage_employee.php.	2.7	More Details
CVE-2026-37596	SourceCodester Online Employees Work From Home Attendance System v1.0 is vulnerable to SQL Injection in the file /wfh_attendance/admin/manage_department.php.	2.7	More Details
CVE-2026-37597	SourceCodester Online Employees Work From Home Attendance System v1.0 is vulnerable to SQL Injection in the file /wfh_attendance/admin/attendance_list.php.	2.7	More Details
CVE-2026-37594	SourceCodester Online Employees Work From Home Attendance System v1.0 is vulnerable to SQL Injection in the file /wfh_attendance/admin/view_employee.php.	2.7	More Details
CVE-2026-37600	SourceCodester Patient Appointment Scheduler System v1.0 is vulnerable to SQL Injection in the file /scheduler/admin/appointments/view_details.php.	2.7	More Details
CVE-2026-37601	SourceCodester Patient Appointment Scheduler System v1.0 is vulnerable to SQL Injection in the file /scheduler/admin/appointments/manage_appointment.php.	2.7	More Details
CVE-2026-37602	SourceCodester Patient Appointment Scheduler System v1.0 is vulnerable to SQL Injection in the file /scheduler/admin/user/manage_user.php.	2.7	More Details
CVE-2026-37593	SourceCodester Online Employees Work From Home Attendance System v1.0 is vulnerable to SQL Injection in the file /wfh_attendance/admin/view_att.php.	2.7	More Details
CVE-2026-37592	Sourcecodester Storage Unit Rental Management System v1.0 is vulnerable to SQL in the file /storage/admin/maintenance/manage_pricing.php.	2.7	More Details
CVE-2026-37591	Sourcecodester Storage Unit Rental Management System v1.0 is vulnerable to SQL injection in the file /storage/admin/tenants/view_details.php.	2.7	More Details
CVE-2026-37590	SourceCodester Storage Unit Rental Management System v1.0 is vulnerable to SQL Injection in the file /storage/admin/rents/manage_rent.php.	2.7	More Details
CVE-2026-37589	SourceCodester Storage Unit Rental Management System v1.0 is vulnerable to SQL Injection in the file /storage/admin/maintenance/manage_storage_unit.php.	2.7	More Details
CVE-2026-34849	UAF vulnerability in the screen management module. Impact: Successful exploitation of this vulnerability may affect availability.	2.5	More Details
CVE-2026-5836	A vulnerability has been found in code-projects Online Shoe Store 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_product.php. The manipulation of the argument product_name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2026-5835	A flaw has been found in code-projects Online Shoe Store 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin_football.php. Executing a manipulation of the argument product_name can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	2.4	More Details

CVE-2026-21006	Improper access control in Samsung DeX prior to SMR Apr-2026 Release 1 allows physical attackers to access to hidden notification contents.	2.4	More Details
CVE-2026-21741	An URL Redirection to Untrusted Site ('Open Redirect') vulnerability [CWE-601] vulnerability in Fortinet FortiNAC-F 7.6.0 through 7.6.5, FortiNAC-F 7.4 all versions, FortiNAC-F 7.2 all versions may allow a remote privileged attacker with system administrator role to redirect users to an arbitrary website via crafted CSV file.	2.4	More Details
CVE-2026-6184	A weakness has been identified in code-projects Simple Content Management System 1.0. This affects an unknown part of the file /web/admin/welcome.php. Executing a manipulation of the argument News Title can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2026-6003	A security vulnerability has been detected in code-projects Simple IT Discussion Forum 1.0. This issue affects some unknown processing of the file /admin/user.php. Such manipulation of the argument fname leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2.4	More Details
CVE-2026-5834	A vulnerability was detected in code-projects Online Shoe Store 1.0. Affected is an unknown function of the file /admin/admin_running.php. Performing a manipulation of the argument product_name results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2.4	More Details
CVE-2026-27308	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. A high-privileged attacker could exploit this vulnerability and exhaust system resources, reducing application speed. Exploitation of this issue does not require user interaction.	2.4	More Details
CVE-2026-27307	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. A high-privileged attacker could exploit this vulnerability and exhaust system resources, reducing application speed. Exploitation of this issue does not require user interaction.	2.4	More Details
CVE-2026-34851	Race condition vulnerability in the event notification module. Impact: Successful exploitation of this vulnerability may affect availability.	2.2	More Details
CVE-2026-27675	SAP Landscape Transformation contains a vulnerability in an RFC-exposed function module that could allow a high privileged adversary to inject arbitrary ABAP code and operating system commands. Due to this, some information could be modified, but the attacker does not have control over kind or degree. This leads to a low impact on integrity, while confidentiality and availability are not impacted.	2.0	More Details
CVE-2026-34850	Race condition vulnerability in the notification service. Impact: Successful exploitation of this vulnerability may affect availability.	1.9	More Details
CVE-2025-66447	Chamilo LMS is a learning management system. From 1.11.0 to 2.0-beta.1, anyone can trigger a malicious redirect through the use of the redirect parameter to /login. This vulnerability is fixed in 2.0-beta.2.	0.0	More Details
CVE-2026-33455	Livestatus injection in the monitoring quicksearch in Checkmk <2.5.0b4 allows an authenticated attacker to inject livestatus commands via the search query due to insufficient input sanitization in search filter plugins.	N/A	More Details
CVE-2026-39416	AIL framework is an open-source platform to collect, crawl, process and analyse unstructured data. Prior to 6.8, a stored cross-site scripting (XSS) vulnerability was identified in the modal item preview functionality. When item content longer than 800 characters was processed, attacker-controlled content was returned without an explicit text/plain content type, allowing the browser to interpret the response as active HTML. This could result in execution of arbitrary JavaScript in the context of an authenticated user viewing a crafted item. This vulnerability is fixed in 6.8.	N/A	More Details
CVE-2026-28704	Emocheck insecurely loads Dynamic Link Libraries (DLLs). If a crafted DLL file is placed to the same directory, an arbitrary code may be executed with the privilege of the user invoking EmoCheck.	N/A	More Details
CVE-2026-1115	A Stored Cross-Site Scripting (XSS) vulnerability was identified in the social feature of parisneo/lollms, affecting the latest version prior to 2.2.0. The vulnerability exists in the `create_post` function within `backend/routers/social/__init__.py`, where user-provided content is directly assigned to the `DBPost` model without sanitization. This allows attackers to inject and store malicious JavaScript, which is executed in the browsers of users viewing the Home Feed, including administrators. This can lead to account takeover, session hijacking, and wormable attacks. The issue is resolved in version 2.2.0.	N/A	More Details
CVE-2026-5477	An integer overflow existed in the wolfCrypt CMAC implementation, that could be exploited to forge CMAC tags. The function wc_CmacUpdate used the guard `if (cmac->totalSz != 0)` to skip XOR-chaining on the first block (where digest is all-zeros and the XOR is a no-op). However, totalSz is word32 and wraps to zero after 2^28 block flushes (4 GiB), causing the guard to erroneously discard the live CBC-MAC chain state. Any two messages sharing a common suffix beyond the 4 GiB mark then produce identical CMAC tags, enabling a zero-work prefix-substitution forgery. The fix removes the guard, making the XOR unconditional; the no-op property on the first block is preserved because digest is zero-initialized by wc_InitCmac_ex.	N/A	More Details
CVE-2026-	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. From 45.0.0 to before 46.0.7, if a non-contiguous buffer was passed to APIs which accepted Python buffers (e.g.	N/A	More Details

39892	Hash.update()), this could lead to buffer overflows. This vulnerability is fixed in 46.0.7.		
CVE-2026-33088	Movable Type provided by Six Apart Ltd. contains an SQL Injection vulnerability which may allow an attacker to execute an arbitrary SQL statement.	N/A	More Details
CVE-2026-35033	Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain an unauthenticated arbitrary file read vulnerability via ffmpeg argument injection through the StreamOptions query parameter parsing mechanism. The ParseStreamOptions method in StreamingHelpers.cs adds any lowercase query parameter to a dictionary without validation, bypassing the RegularExpression attribute on the level controller parameter, and the unsanitized value is concatenated directly into the ffmpeg command line. By injecting a drawtext filter with a textfile argument, an attacker can read arbitrary server files such as /etc/shadow and exfiltrate their contents as text rendered in the video stream response. The vulnerable /Videos/{itemId}/stream endpoint has no Authorize attribute, making this exploitable without authentication, though item GUIDs are pseudorandom and require an authenticated user to obtain. This issue has been fixed in version 10.11.7.	N/A	More Details
CVE-2026-4482	The installer certificate files in the .../bootstrap/common/ssl folder do not seem to have restricted permissions on Windows systems (users have read and execute access). For the client.key file in particular, this could potentially lead to exploits, as this exposes agent identity material to any locally authenticated standard user.	N/A	More Details
CVE-2026-4112	Improper neutralization of special elements used in an SQL command (“SQL Injection”) in SonicWall SMA1000 series appliances allows a remote authenticated attacker with read-only administrator privileges to escalate privileges to primary administrator.	N/A	More Details
CVE-2026-5501	wolfSSL_X509_verify_cert in the OpenSSL compatibility layer accepts a certificate chain in which the leaf's signature is not checked, if the attacker supplies an untrusted intermediate with Basic Constraints `CA:FALSE` that is legitimately signed by a trusted root. An attacker who obtains any leaf certificate from a trusted CA (e.g. a free DV cert from Let's Encrypt) can forge a certificate for any subject name with any public key and arbitrary signature bytes, and the function returns `WOLFSSL_SUCCESS` / `X509_V_OK`. The native wolfSSL TLS handshake path (`ProcessPeerCerts`) is not susceptible and the issue is limited to applications using the OpenSSL compatibility API directly, which would include integrations of wolfSSL into nginx and haproxy.	N/A	More Details
CVE-2026-33457	Livestatus injection in the prediction graph page in Checkmk <2.5.0b4, <2.4.0p26, and <2.3.0p47 allows an authenticated user to inject arbitrary Livestatus commands via a crafted service name parameter due to insufficient sanitization of the service description value.	N/A	More Details
CVE-2026-25776	Movable Type provided by Six Apart Ltd. contains a code injection vulnerability which may allow an attacker to execute arbitrary Perl script.	N/A	More Details
CVE-2026-40074	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to 2.57.1, redirect, when called from inside the handle server hook with a location parameter containing characters that are invalid in a HTTP header, will cause an unhandled TypeError. This could result in DoS on some platforms, especially if the location passed to redirect contains unsanitized user input. This vulnerability is fixed in 2.57.1.	N/A	More Details
CVE-2026-4901	Hydrosystem Control System saves sensitive information into a log file. Critically, user credentials are logged allowing the attacker to obtain further authorized access into the system. Combined with vulnerability CVE-2026-34184, these sensitive information could be accessed by an unauthorized user.This issue was fixed in Hydrosystem Control System version 9.8.5	N/A	More Details
CVE-2026-40157	PraisonAI is a multi-agent teams system. Prior to 4.5.128, cmd_unpack in the recipe CLI extracts .praison tar archives using raw tar.extract() without validating archive member paths. A .praison bundle containing ../../ entries will write files outside the intended output directory. An attacker who distributes a malicious bundle can overwrite arbitrary files on the victim's filesystem when they run praisonai recipe unpack. This vulnerability is fixed in 4.5.128.	N/A	More Details
CVE-2026-34718	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, the HTML sanitizer for ticket articles was missing proper sanitization of data: ... URI schemes, resulting in storing such malicious content in the database of the Zammad instance. The Zammad GUI is rendering this content, due to applied CSP rules no harm was done by e.g., clicking such a link. This vulnerability is fixed in 7.0.1 and 6.5.4.	N/A	More Details
CVE-2026-5500	wolfSSL's wc_PKCS7_DecodeAuthEnvelopedData() does not properly sanitize the AES-GCM authentication tag length received and has no lower bounds check. A man-in-the-middle can therefore truncate the mac field from 16 bytes to 1 byte, reducing the tag check from 2^{-128} to 2^{-8}.	N/A	More Details
CVE-2026-40160	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, web_crawl's httpx fallback path passes user-supplied URLs directly to httpx.AsyncClient.get() with follow_redirects=True and no host validation. An LLM agent tricked into crawling an internal URL can reach cloud metadata endpoints (169.254.169.254), internal services, and localhost. The response content is returned to the agent and may appear in output visible to the attacker. This fallback is the default crawl path on a fresh PraisonAI installation (no Tavily key, no Crawl4AI installed). This vulnerability is fixed in 1.5.128.	N/A	More Details
CVE-2026-34248	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1, customers in shared organizations (means they can see each other's tickets) could see fields which are not intended for customers - including fields not intended for them at all (e.g. priority, custom ticket attributes for internal purposes). This was the case when a customer opened a ticket from another user of the same shared organization. They are not able to modify these field. This vulnerability is fixed in 7.0.1.	N/A	More Details
CVE-	In wolfSSL's EVP layer, the ChaCha20-Poly1305 AEAD decryption path in wolfSSL_EVP_CipherFinal (and related EVP		

2026-5479	cipher finalization functions) fails to verify the authentication tag before returning plaintext to the caller. When an application uses the EVP API to perform ChaCha20-Poly1305 decryption, the implementation computes or accepts the tag but does not compare it against the expected value.	N/A	More Details
CVE-2026-33456	Livestatus injection in the notification test mode in Checkmk <2.5.0b4 and <2.4.0p26 allows an authenticated user with access to the notification test page to inject arbitrary Livestatus commands via a crafted service description.	N/A	More Details
CVE-2026-40073	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to 2.57.1, under certain circumstances, requests could bypass the BODY_SIZE_LIMIT on SvelteKit applications running with adapter-node. This bypass does not affect body size limits at other layers of the application stack, so limits enforced in the WAF, gateway, or at the platform level are unaffected. This vulnerability is fixed in 2.57.1.	N/A	More Details
CVE-2026-34782	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, the REST endpoint POST /api/v1/ai_assistance/text_tools/:id was not checking if a user is privileged to use the text tool, resulting in being able to use it in all situations. This vulnerability is fixed in 7.0.1 and 6.5.4.	N/A	More Details
CVE-2026-34480	Apache Log4j Core's XmlLayout https://logging.apache.org/log4j/2.x/manual/layouts.html#XmlLayout , in versions up to and including 2.25.3, fails to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets producing invalid XML output whenever a log message or MDC value contains such characters. The impact depends on the StAX implementation in use: * JRE built-in StAX: Forbidden characters are silently written to the output, producing malformed XML. Conforming parsers must reject such documents with a fatal error, which may cause downstream log-processing systems to drop the affected records. * Alternative StAX implementations (e.g., Woodstox https://github.com/FasterXML/woodstox , a transitive dependency of the Jackson XML Dataformat module): An exception is thrown during the logging call, and the log event is never delivered to its intended appender, only to Log4j's internal status logger. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue by sanitizing forbidden characters before XML output.	N/A	More Details
CVE-2026-34724	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1, a server-side template injection vulnerability which leads to RCE via AI Agent exists. Impact is limited to environments where an attacker can control or influence type_enrichment_data (typically high-privilege administrative configuration). This vulnerability is fixed in 7.0.1.	N/A	More Details
CVE-2026-33414	Podman is a tool for managing OCI containers and pods. Versions 4.8.0 through 5.8.1 contain a command injection vulnerability in the HyperV machine backend in pkg/machine/hyperv/stubber.go, where the VM image path is inserted into a PowerShell double-quoted string without sanitization, allowing $() subexpression injection. Because PowerShell evaluates subexpressions inside double-quoted strings before executing the outer command, an attacker who can control the VM image path through a crafted machine name or image directory can execute arbitrary PowerShell commands with the privileges of the Podman process. On typical Windows installations this means SYSTEM-level code execution, and only Windows is affected as the code is exclusive to the HyperV backend. This issue has been patched in version 5.8.2.	N/A	More Details
CVE-2026-34837	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1, he REST endpoint POST /api/v1/ai_assistance/text_tools/:id contains an authorization failure. Context data (e.g., a group or organization) supplied to be used in the AI prompt were not checked if they are accessible for the current user. This leads to having data present in the AI prompt that were not authorized before being used. A user needs to have ticket.agent permission to be able to use the provided context data. This vulnerability is fixed in 7.0.1.	N/A	More Details
CVE-2026-4114	Improper handling of Unicode encoding in SonicWall SMA1000 series appliances allows a remote authenticated SSLVPN admin to bypass AMC TOTP authentication.	N/A	More Details
CVE-2026-34185	Hydrosystem Control System is vulnerable to SQL Injection across most scripts and input parameters. Because no protections are in place, an authenticated attacker can inject arbitrary SQL commands, potentially gaining full control over the database.This issue was fixed in Hydrosystem Control System version 9.8.5	N/A	More Details
CVE-2026-34184	Hydrosystem Control System does not enforce authorization for some directories. This allows an unauthorized attacker to read all files in these directories and even execute some of them. Critically the attacker could run PHP scripts directly on the connected database.This issue was fixed in Hydrosystem Control System version 9.8.5	N/A	More Details
CVE-2026-40023	Apache Log4cxx's XMLLayout https://logging.apache.org/log4cxx/1.7.0/classlog4cxx_1_1xml_1_1XMLLayout.html , in versions before 1.7.0, fails to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets in log messages, NDC, and MDC property keys and values, producing invalid XML output. Conforming XML parsers must reject such documents with a fatal error, which may cause downstream log processing systems to drop or fail to index affected records. An attacker who can influence logged data can exploit this to suppress individual log records, impairing audit trails and detection of malicious activity. Users are advised to upgrade to Apache Log4cxx 1.7.0, which fixes this issue.	N/A	More Details
CVE-2026-39486	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Chill Download Monitor download-monitor allows Blind SQL Injection.This issue affects Download Monitor: from n/a through <= 5.1.8.	N/A	More Details
CVE-2026-	Apache Log4net's XmlLayout https://logging.apache.org/log4net/manual/configuration/layouts.html#layout-list and XmlLayoutSchemaLog4J https://logging.apache.org/log4net/manual/configuration/layouts.html#layout-list , in versions before 3.3.0, fail to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets in MDC property keys and values, as well as the identity field that may carry attacker-influenced data. This causes an exception during serialization and the silent loss of the affected log event.	N/A	More Details

40021	An attacker who can influence any of these fields can exploit this to suppress individual log records, impairing audit trails and detection of malicious activity. Users are advised to upgrade to Apache Log4net 3.3.0, which fixes this issue.		
CVE-2026-34481	Apache Log4j's JsonTemplateLayout https://logging.apache.org/log4j/2.x/manual/json-template-layout.html , in versions up to and including 2.25.3, produces invalid JSON output when log events contain non-finite floating-point values (NaN, Infinity, or -Infinity), which are prohibited by RFC 8259. This may cause downstream log processing systems to reject or fail to index affected records. An attacker can exploit this issue only if both of the following conditions are met: * The application uses JsonTemplateLayout. * The application logs a MapMessage containing an attacker-controlled floating-point value. Users are advised to upgrade to Apache Log4j JSON Template Layout 2.25.4, which corrects this issue.	N/A	More Details
CVE-2026-34722	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, the used endpoint for ticket creation was missing authorization if the related parameter for adding links is used. This vulnerability is fixed in 7.0.1 and 6.5.4.	N/A	More Details
CVE-2026-34479	The Log4j1XmlLayout from the Apache Log4j 1-to-Log4j 2 bridge fails to escape characters forbidden by the XML 1.0 standard, producing malformed XML output. Conforming XML parsers are required to reject documents containing such characters with a fatal error, which may cause downstream log processing systems to drop or fail to index affected records. Two groups of users are affected: * Those using Log4j1XmlLayout directly in a Log4j Core 2 configuration file. * Those using the Log4j 1 configuration compatibility layer with org.apache.log4j.xml.XMLLayout specified as the layout class. Users are advised to upgrade to Apache Log4j 1-to-Log4j 2 bridge version 2.25.4, which corrects this issue. Note: The Apache Log4j 1-to-Log4j 2 bridge is deprecated and will not be present in Log4j 3. Users are encouraged to consult the Log4j 1 to Log4j 2 migration guide https://logging.apache.org/log4j/2.x/migrate-from-log4j1.html , and specifically the section on eliminating reliance on the bridge.	N/A	More Details
CVE-2026-35032	Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chain in the LiveTV M3U tuner endpoint (POST /LiveTv/TunerHosts), where the tuner URL is not validated, allowing local file read via non-HTTP paths and Server-Side Request Forgery (SSRF) via HTTP URLs. This is exploitable by any authenticated user because the EnableLiveTvManagement permission defaults to true for all new users. An attacker can chain these vulnerabilities by adding an M3U tuner pointing to an attacker-controlled server, serving a crafted M3U with a channel pointing to the Jellyfin database, exfiltrating the database to extract admin session tokens, and escalating to admin privileges. This issue has been fixed in version 10.11.7. If users are unable to upgrade immediately, they can disable Live TV Management privileges for all users.	N/A	More Details
CVE-2026-34478	Apache Log4j Core's Rfc5424Layout https://logging.apache.org/log4j/2.x/manual/layouts.html#RFC5424Layout , in versions 2.21.0 through 2.25.3, is vulnerable to log injection via CRLF sequences due to undocumented renames of security-relevant configuration attributes. Two distinct issues affect users of stream-based syslog services who configure Rfc5424Layout directly: * The newLineEscape attribute was silently renamed, causing newline escaping to stop working for users of TCP framing (RFC 6587), exposing them to CRLF injection in log output. * The useTlsMessageFormat attribute was silently renamed, causing users of TLS framing (RFC 5425) to be silently downgraded to unframed TCP (RFC 6587), without newline escaping. Users of the SyslogAppender are not affected, as its configuration attributes were not modified. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue.	N/A	More Details
CVE-2026-34477	The fix for CVE-2025-68161 https://logging.apache.org/security.html#CVE-2025-68161 was incomplete: it addressed hostname verification only when enabled via the log4j2.sslVerifyHostName https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property, but not when configured through the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName attribute of the <Ssl> element. Although the verifyHostName configuration attribute was introduced in Log4j Core 2.12.0, it was silently ignored in all versions through 2.25.3, leaving TLS connections vulnerable to interception regardless of the configured value. A network-based attacker may be able to perform a man-in-the-middle attack when all of the following conditions are met: * An SMTP, Socket, or Syslog appender is in use. * TLS is configured via a nested <Ssl> element. * The attacker can present a certificate issued by a CA trusted by the appender's configured trust store, or by the default Java trust store if none is configured. This issue does not affect users of the HTTP appender, which uses a separate verifyHostname https://logging.apache.org/log4j/2.x/manual/appenders/network.html#HttpAppender-attr-verifyHostName attribute that was not subject to this bug and verifies host names by default. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue.	N/A	More Details
CVE-2026-39851	Saleor is an e-commerce platform. From 2.10.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, the requestEmailChange() mutation was revealing the existence of user-provided email addresses in error messages. This vulnerability is fixed in 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118.	N/A	More Details
CVE-2026-5466	wolfSSL's ECCSI signature verifier `wc_VerifyEccsiHash` decodes the `r` and `s` scalars from the signature blob via `mp_read_unsigned_bin` with no check that they lie in `[1, q-1]`. A crafted forged signature could verify against any message for any identity, using only publicly-known constants.	N/A	More Details
CVE-2026-5774	Improper synchronization of the userTokens map in the API server in Canonical Juju 4.0.5, 3.6.20, and 2.9.56 may allow an authenticated user to possibly cause a denial of service on the server or possibly reuse a single-use discharge token.	N/A	More Details
CVE-2026-5777	This vulnerability exists in the Atom 3x Projector due to improper exposure of the Android Debug Bridge (ADB) service over the local network without authentication or access controls. An unauthenticated attacker on the same network can exploit this vulnerability to obtain root-level access, leading to complete compromise of the targeted device.	N/A	More Details

CVE-2026-34721	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, the OAuth callback endpoints for Microsoft, Google, and Facebook external credentials do not validate a CSRF state parameter. This vulnerability is fixed in 7.0.1 and 6.5.4.	N/A	More Details
CVE-2026-39862	Tophat is a mobile applications testing harness. Prior to 2.5.1, Tophat is affected by remote code execution via crafted tophat:// or http://localhost:29070 URLs. The arguments query parameter flows unsanitized from URL parsing through to /bin/bash -c execution, allowing an attacker to execute arbitrary commands on a developer's macOS workstation. Any developer with Tophat installed is vulnerable. For previously trusted build hosts, no confirmation dialog appears. Attacker commands run with the user's permissions. This vulnerability is fixed in 2.5.1.	N/A	More Details
CVE-2026-31412	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_mass_storage: Fix potential integer overflow in check_command_size_in_blocks() The `check_command_size_in_blocks()` function calculates the data size in bytes by left shifting `common->data_size_from_cmnd` by the block size (`common->curlun->blkbits`). However, it does not validate whether this shift operation will cause an integer overflow. Initially, the block size is set up in `fsg_lun_open()` , and the `common->data_size_from_cmnd` is set up in `do_scsi_command()`. During initialization, there is no integer overflow check for the interaction between two variables. So if a malicious USB host sends a SCSI READ or WRITE command requesting a large amount of data (`common->data_size_from_cmnd`), the left shift operation can wrap around. This results in a truncated data size, which can bypass boundary checks and potentially lead to memory corruption or out-of-bounds accesses. Fix this by using the check_shl_overflow() macro to safely perform the shift and catch any overflows.	N/A	More Details
CVE-2026-34720	Zammad is a web based open source helpdesk/customer support system. Prior to 7.0.1 and 6.5.4, the SSO mechanism in Zammad was not verifying the header originates from a trusted SSO proxy/gateway before applying further actions on it. This vulnerability is fixed in 7.0.1 and 6.5.4.	N/A	More Details
CVE-2026-39414	MinIO is a high-performance object storage system. From RELEASE.2018-08-18T03-49-57Z to before RELEASE.2025-12-20T04-58-37Z, MinIO's S3 Select feature is vulnerable to memory exhaustion when processing CSV files containing lines longer than available memory. The CSV reader's nextSplit() function calls bufio.Reader.ReadBytes('\n') with no size limit, buffering the entire input in memory until a newline is found. A CSV file with no newline characters causes the entire contents to be read into a single allocation, leading to an OOM crash of the MinIO server process. This is exploitable by any authenticated user with s3:PutObject and s3:GetObject permissions. The attack is especially practical when combined with compression: a ~2 MB gzip-compressed CSV can decompress to gigabytes of data without newlines, allowing a small upload to cause large memory consumption on the server. However, compression is not required — a sufficiently large uncompressed CSV with no newlines triggers the same issue.	N/A	More Details
CVE-2026-39362	InvenTree is an Open Source Inventory Management System. Prior to 1.2.7 and 1.3.0, when INVENTREE_DOWNLOAD_FROM_URL is enabled (opt-in), authenticated users can supply remote_image URLs that are fetched server-side via requests.get() with only Django's URLValidator check. There is no validation against private IP ranges or internal hostnames. Redirects are followed (allow_redirects=True), enabling bypass of any URL-format checks. This vulnerability is fixed in 1.2.7 and 1.3.0.	N/A	More Details
CVE-2026-34941	Wasmtime is a runtime for WebAssembly. Prior to 24.0.7, 36.0.7, 42.0.2, and 43.0.1, Wasmtime contains a vulnerability where when transcoding a UTF-16 string to the latin1+utf16 component-model encoding it would incorrectly validate the byte length of the input string when performing a bounds check. Specifically the number of code units were checked instead of the byte length, which is twice the size of the code units. This vulnerability can cause the host to read beyond the end of a WebAssembly's linear memory in an attempt to transcode nonexistent bytes. In Wasmtime's default configuration this will read unmapped memory on a guard page, terminating the process with a segfault. Wasmtime can be configured, however, without guard pages which would mean that host memory beyond the end of linear memory may be read and interpreted as UTF-16. A host segfault is a denial-of-service vulnerability in Wasmtime, and possibly being able to read beyond the end of linear memory is additionally a vulnerability. Note that reading beyond the end of linear memory requires nonstandard configuration of Wasmtime, specifically with guard pages disabled. This vulnerability is fixed in 24.0.7, 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-5188	An integer underflow issue exists in wolfSSL when parsing the Subject Alternative Name (SAN) extension of X.509 certificates. A malformed certificate can specify an entry length larger than the enclosing sequence, causing the internal length counter to wrap during parsing. This results in incorrect handling of certificate data. The issue is limited to configurations using the original ASN.1 parsing implementation which is off by default.	N/A	More Details
CVE-2026-24913	SQL Injection vulnerability exists in MATCHA INVOICE 2.6.6 and earlier. If this vulnerability is exploited, information stored in the database may be obtained or altered by a user who can log in to the product.	N/A	More Details
CVE-2026-39972	Mercure is a protocol for pushing data updates to web browsers and other HTTP clients in a battery-efficient way. Prior to 0.22.0, a cache key collision vulnerability in TopicSelectorStore allows an attacker to poison the match result cache, potentially causing private updates to be delivered to unauthorized subscribers or blocking delivery to authorized ones. The cache key was constructed by concatenating the topic selector and topic with an underscore separator. Because both topic selectors and topics can contain underscores, two distinct pairs can produce the same key. An attacker who can subscribe to the hub or publish updates with crafted topic names can exploit this to bypass authorization checks on private updates. This vulnerability is fixed in 0.22.0.	N/A	More Details
CVE-2026-5194	Missing hash/digest size and OID checks allow digests smaller than allowed when verifying ECDSA certificates, or smaller than is appropriate for the relevant key type, to be accepted by signature verification functions. This could lead to reduced security of ECDSA certificate-based authentication if the public CA key used is also known. This affects ECDSA/ECC verification when EdDSA or ML-DSA is also enabled.	N/A	More Details

CVE-2026-5187	Two potential heap out-of-bounds write locations existed in DecodeObjectId() in wolfcrypt/src/asn.c. First, a bounds check only validates one available slot before writing two OID arc values (out[0] and out[1]), enabling a 2-byte out-of-bounds write when outSz equals 1. Second, multiple callers pass sizeof(decOid) (64 bytes on 64-bit platforms) instead of the element count MAX_OID_SZ (32), causing the function to accept crafted OIDs with 33 or more arcs that write past the end of the allocated buffer.	N/A	More Details
CVE-2026-39977	flatpak-builder is a tool to build flatpaks from source. From 1.4.5 to before 1.4.8, the license-files manifest key takes an array of paths to user defined licence files relative to the source directory of the module. The paths from that array are resolved using g_file_resolve_relative_path() and validated to stay inside the source directory using two checks - g_file_get_relative_path() which does not resolve symlinks and g_file_query_file_type() with G_FILE_QUERY_INFO_NOFOLLOW_SYMLINKS which only applies to the final path component. The copy operation runs on host. This can be exploited by using a crafted manifest and/or source to read arbitrary files from the host and capture them into the build output. This vulnerability is fixed in 1.4.8.	N/A	More Details
CVE-2026-35063	OpenPLC_V3 REST API endpoint checks for JWT presence but never verifies the caller's role. Any authenticated user with role=user can delete any other user, including administrators, by specifying their user ID or they can create new accounts with role=admin, escalating to full administrator access.	N/A	More Details
CVE-2026-3199	A vulnerability in the task management component of Sonatype Nexus Repository versions 3.22.1 through 3.90.2 allows an authenticated attacker with task creation permissions to execute arbitrary code, bypassing the nexus.scripts.allowCreation security control.	N/A	More Details
CVE-2026-33273	Unrestricted upload of file with dangerous type issue exists in MATCHA INVOICE 2.6.6 and earlier. If this vulnerability is exploited, an arbitrary file may be created by an administrator of the product. As a result, arbitrary code may be executed on the server.	N/A	More Details
CVE-2026-3438	A reflected cross-site scripting vulnerability exists in Sonatype Nexus Repository versions 3.0.0 through 3.90.2 that allows unauthenticated remote attackers to execute arbitrary JavaScript in a victim's browser through a specially crafted URL. Exploitation requires user interaction.	N/A	More Details
CVE-2026-25133	October is a Content Management System (CMS) and web platform. Versions prior to 3.7.14 and 4.1.10 contain a stored cross-site scripting (XSS) vulnerability in the SVG sanitization logic. The regex pattern used to strip event handler attributes (such as onclick or onload) could be bypassed using a crafted payload that exploits how the pattern matches attribute boundaries, allowing malicious SVG files to be uploaded through the Media Manager with embedded JavaScript. Exploitation could lead to privilege escalation if a superuser views or embeds the malicious SVG, and requires authenticated backend access with media upload permissions. The SVG must be viewed or embedded in a page for the payload to trigger. This issue has been fixed in versions 3.7.14 and 4.1.10.	N/A	More Details
CVE-2026-27787	Cross-site scripting vulnerability exists in MATCHA SNS 1.3.9 and earlier. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the website using the product.	N/A	More Details
CVE-2026-39907	Unisys WebPerfect Image Suite versions 3.0.3960.22810 and 3.0.3960.22604 expose an unauthenticated WCF SOAP endpoint on TCP port 1208 that accepts unsanitized file paths in the ReadLicense action's LFName parameter, allowing remote attackers to trigger SMB connections and leak NTLMv2 machine-account hashes. Attackers can submit crafted SOAP requests with UNC paths to force the server to initiate outbound SMB connections, exposing authentication credentials that may be relayed for privilege escalation or lateral movement within the network.	N/A	More Details
CVE-2026-39906	Unisys WebPerfect Image Suite versions 3.0.3960.22810 and 3.0.3960.22604 expose a deprecated .NET Remoting TCP channel that allows remote unauthenticated attackers to leak NTLMv2 machine-account hashes by supplying a Windows UNC path as a target file argument through object-unmarshalling techniques. Attackers can capture the leaked NTLMv2 hash and relay it to other hosts to achieve privilege escalation or lateral movement depending on network configuration and patch level.	N/A	More Details
CVE-2026-33714	Chamilo is an open-source learning management system (LMS). Version 2.0.0-RC.2 contains a SQL Injection vulnerability in the statistics AJAX endpoint, which is an incomplete fix for CVE-2026-30881. While CVE-2026-30881 was patched by applying Security::remove_XSS() to the date_start and date_end parameters in the get_user_registration_by_month action, the same parameters remain unsanitized in the users_active action within the same file (public/main/inc/ajax/statistics.ajax.php), where they are directly interpolated into a SQL query. An authenticated admin can exploit this to perform time-based blind SQL injection, enabling extraction of arbitrary data from the database. This issue has been fixed in version 2.0.0.	N/A	More Details
CVE-2026-35556	OpenPLC_V3 is vulnerable to a Plaintext Storage of a Password vulnerability that could allow an attacker to retrieve credentials and access sensitive information.	N/A	More Details
CVE-2026-4483	An exposed IOCTL with an insufficient access control vulnerability has been identified in the utility, MxGeneralIo, for Moxa’s industrial x86 computers. The affected utility, MxGeneralIo, exposes IOCTL methods that permit direct read and write access to MSR and system memory. A local attacker with high privileges could abuse these interfaces to perform unauthorized operations. Successful exploitation may result in privilege escalation on Windows 7 systems or cause a system crash (BSoD) on Windows 10 and 11 systems, leading to a denial-of-service condition. The vulnerability could slightly affect the confidentiality and integrity of the device, but availability might be heavily impacted. No impact to the subsequent system has been identified.	N/A	More Details
CVE-	marimo is a reactive Python notebook. Prior to 0.23.0, Marimo has a Pre-Auth RCE vulnerability. The terminal WebSocket endpoint /terminal/ws lacks authentication validation, allowing an unauthenticated attacker to obtain a		

2026-39987	full PTY shell and execute arbitrary system commands. Unlike other WebSocket endpoints (e.g., /ws) that correctly call validate_auth() for authentication, the /terminal/ws endpoint only checks the running mode and platform support before accepting connections, completely skipping authentication verification. This vulnerability is fixed in 0.23.0.	N/A	More Details
CVE-2026-34161	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in the social post attachment upload functionality, where an authenticated user can upload a malicious HTML file containing JavaScript via the /api/social_post_attachments endpoint. The uploaded file is served back from the application at the generated contentUrl without sanitization, content type restrictions, or a Content-Disposition: attachment header, causing the JavaScript to execute in the browser within the application's origin. Because the payload is stored server-side and runs in the trusted origin, an attacker can perform session hijacking, account takeover, privilege escalation (if an admin views the link), and arbitrary actions on behalf of the victim. This issue has been fixed in version 2.0.0-RC.3.	N/A	More Details
CVE-2026-35195	Wasmtime is a runtime for WebAssembly. Prior to 24.0.7, 36.0.7, 42.0.2, and 43.0.1, Wasmtime's implementation of transcoding strings between components contains a bug where the return value of a guest component's realloc is not validated before the host attempts to write through the pointer. This enables a guest to cause the host to write arbitrary transcoded string bytes to an arbitrary location up to 4GiB away from the base of linear memory. These writes on the host could hit unmapped memory or could corrupt host data structures depending on Wasmtime's configuration. Wasmtime by default reserves 4GiB of virtual memory for a guest's linear memory meaning that this bug will by default on hosts cause the host to hit unmapped memory and abort the process due to an unhandled fault. Wasmtime can be configured, however, to reserve less memory for a guest and to remove all guard pages, so some configurations of Wasmtime may lead to corruption of data outside of a guest's linear memory, such as host data structures or other guests's linear memories. This vulnerability is fixed in 24.0.7, 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-4398	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-34988	Wasmtime is a runtime for WebAssembly. From 28.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime's implementation of its pooling allocator contains a bug where in certain configurations the contents of linear memory can be leaked from one instance to the next. The implementation of resetting the virtual memory permissions for linear memory used the wrong predicate to determine if resetting was necessary, where the compilation process used a different predicate. This divergence meant that the pooling allocator incorrectly deduced at runtime that resetting virtual memory permissions was not necessary while compile-time determine that virtual memory could be relied upon. The pooling allocator must be in use, Config::memory_guard_size configuration option must be 0, Config::memory_reservation configuration must be less than 4GiB, and pooling allocator must be configured with max_memory_size the same as the memory_reservation value in order to exploit this vulnerability. If all of these conditions are applicable then when a linear memory is reused the VM permissions of the previous iteration are not reset. This means that the compiled code, which is assuming out-of-bounds loads will segfault, will not actually segfault and can read the previous contents of linear memory if it was previously mapped. This represents a data leakage vulnerability between guest WebAssembly instances which breaks WebAssembly's semantics and additionally breaks the sandbox that Wasmtime provides. Wasmtime is not vulnerable to this issue with its default settings, nor with the default settings of the pooling allocator, but embeddings are still allowed to configure these values to cause this vulnerability. This vulnerability is fixed in 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-34987	Wasmtime is a runtime for WebAssembly. From 25.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime with its Winch (baseline) non-default compiler backend may allow properly constructed guest Wasm to access host memory outside of its linear-memory sandbox. This vulnerability requires use of the Winch compiler (-Ccompiler=winch). By default, Wasmtime uses its Cranelift backend, not Winch. With Winch, the same incorrect assumption is present in theory on both aarch64 and x86-64. The aarch64 case has an observed-working proof of concept, while the x86-64 case is theoretical and may not be reachable in practice. This Winch compiler bug can allow the Wasm guest to access memory before or after the linear-memory region, independently of whether pre- or post-guard regions are configured. The accessible range in the initial bug proof-of-concept is up to 32KiB before the start of memory, or ~4GiB after the start of memory, independently of the size of pre- or post-guard regions or the use of explicit or guard-region-based bounds checking. However, the underlying bug assumes a 32-bit memory offset stored in a 64-bit register has its upper bits cleared when it may not, and so closely related variants of the initial proof-of-concept may be able to access truly arbitrary memory in-process. This could result in a host process segmentation fault (DoS), an arbitrary data leak from the host process, or with a write, potentially an arbitrary RCE. This vulnerability is fixed in 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-34983	Wasmtime is a runtime for WebAssembly. In 43.0.0, cloning a wasmtime::Linker is unsound and can result in use-after-free bugs. This bug is not controllable by guest Wasm programs. It can only be triggered by a specific sequence of embedder API calls made by the host. Specifically, the following steps must occur to trigger the bug clone a wasmtime::Linker, drop the original linker instance, use the new, cloned linker instance, resulting in a use-after-free. This vulnerability is fixed in 43.0.1.	N/A	More Details
CVE-2026-40072	web3.py allows you to interact with the Ethereum blockchain using Python. From 6.0.0b3 to before 7.15.0 and 8.0.0b2, web3.py implements CCIP Read / OffchainLookup (EIP-3668) by performing HTTP requests to URLs supplied by smart contracts in offchain_lookup_payload["urls"]. The implementation uses these contract-supplied URLs directly (after {sender} / {data} template substitution) without any destination validation. CCIP Read is enabled by default (global_ccip_read_enabled = True on all providers), meaning any application using web3.py's .call() method is exposed without explicit opt-in. This results in Server-Side Request Forgery (SSRF) when web3.py is used in backend services, indexers, APIs, or any environment that performs eth_call / .call() against untrusted or user-supplied contract addresses. A malicious contract can force the web3.py process to issue HTTP requests to arbitrary	N/A	More Details

	destinations, including internal network services and cloud metadata endpoints. This vulnerability is fixed in 7.15.0 and 8.0.0b2.		
CVE-2026-34946	Wasmtime is a runtime for WebAssembly. From 25.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime's Winch compiler contains a vulnerability where the compilation of the table.fill instruction can result in a host panic. This means that a valid guest can be compiled with Winch, on any architecture, and cause the host to panic. This represents a denial-of-service vulnerability in Wasmtime due to guests being able to trigger a panic. The specific issue is that a historical refactoring changed how compiled code referenced tables within the table.* instructions. This refactoring forgot to update the Winch code paths associated as well, meaning that Winch was using the wrong indexing scheme. Due to the feature support of Winch the only problem that can result is tables being mixed up or nonexistent tables being used, meaning that the guest is limited to panicking the host (using a nonexistent table), or executing spec-incorrect behavior and modifying the wrong table. This vulnerability is fixed in 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-28205	OpenPLC_V3 is vulnerable to an Initialization of a Resource with an Insecure Default vulnerability which could allow an attacker to gain access to the system by bypassing authentication via an API.	N/A	More Details
CVE-2026-34945	Wasmtime is a runtime for WebAssembly. From 25.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime's Winch compiler contains a bug where a 64-bit table, part of the memory64 proposal of WebAssembly, incorrectly translated the table.size instruction. This bug could lead to disclosing data on the host's stack to WebAssembly guests. The host's stack can possibly contain sensitive data related to other host-originating operations which is not intended to be disclosed to guests. This bug specifically arose from a mistake where the return value of table.size was statically typed as a 32-bit integer, as opposed to consulting the table's index type to see how large the returned register could be. When combined with details about Wnich's ABI, such as multi-value returns, this can be combined to read stack data from the host, within a guest. This vulnerability is fixed in 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-34944	Wasmtime is a runtime for WebAssembly. Prior to 24.0.7, 36.0.7, 42.0.2, and 43.0.1, On x86-64 platforms with SSE3 disabled Wasmtime's compilation of the f64x2.splat WebAssembly instruction with Cranelift may load 8 more bytes than is necessary. When signals-based-traps are disabled this can result in a uncaught segfault due to loading from unmapped guard pages. With guard pages disabled it's possible for out-of-sandbox data to be loaded, but this data is not visible to WebAssembly guests. This vulnerability is fixed in 24.0.7, 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-34943	Wasmtime is a runtime for WebAssembly. Prior to 24.0.7, 36.0.7, 42.0.2, and 43.0.1, Wasmtime contains a possible panic which can happen when a flags-typed component model value is lifted with the Val type. If bits are set outside of the set of flags the component model specifies that these bits should be ignored but Wasmtime will panic when this value is lifted. This panic only affects wasmtime's implementation of lifting into Val, not when using the flags! macro. This additionally only affects flags-typed values which are part of a WIT interface. This has the risk of being a guest-controlled panic within the host which Wasmtime considers a DoS vector. This vulnerability is fixed in 24.0.7, 36.0.7, 42.0.2, and 43.0.1.	N/A	More Details
CVE-2026-35206	Helm is a package manager for Charts for Kubernetes. In Helm versions <=3.20.1 and <=4.1.3, a specially crafted Chart will cause helm pull --untar [chart URL | repo/chartname] to write the Chart's contents to the immediate output directory (as defaulted to the current working directory; or as given by the --destination and --untardir flags), rather than the expected output directory suffixed by the chart's name. This vulnerability is fixed in 3.20.2 and 4.1.4.	N/A	More Details
CVE-2026-40107	SiYuan is a personal knowledge management system. Prior to 3.6.4, SiYuan configures Mermaid.js with securityLevel: "loose" and htmlLabels: true. In this mode, <img> tags with src attributes survive Mermaid's internal DOMPurify and land in SVG <foreignObject> blocks. The SVG is injected via innerHTML with no secondary sanitization. When a victim opens a note containing a malicious Mermaid diagram, the Electron client fetches the URL. On Windows, a protocol-relative URL (//attacker.com/image.png) resolves as a UNC path (\\attacker.com\image.png). Windows attempts SMB authentication automatically, sending the victim's NTLMv2 hash to the attacker. This vulnerability is fixed in 3.6.4.	N/A	More Details
CVE-2026-39962	MISP is an open source threat intelligence and sharing platform. Prior to 2.5.36, improper neutralization of special elements in an LDAP query in ApacheAuthenticate.php allows LDAP injection via an unsanitized username value when ApacheAuthenticate.apacheEnv is configured to use a user-controlled server variable instead of REMOTE_USER (such as in certain proxy setups). An attacker able to control that value can manipulate the LDAP search filter and potentially bypass authentication constraints or cause unauthorized LDAP queries. This vulnerability is fixed in 2.5.36.	N/A	More Details
CVE-2026-1163	An insufficient session expiration vulnerability exists in the latest version of parisneo/lollms. The application fails to invalidate active sessions after a password reset, allowing an attacker to continue using an old session token. This issue arises due to the absence of logic to reject requests after a period of inactivity and the excessively long default session duration of 31 days. The vulnerability enables an attacker to maintain persistent access to a compromised account, even after the victim resets their password.	N/A	More Details
CVE-2026-5460	A heap use-after-free exists in wolfSSL's TLS 1.3 post-quantum cryptography (PQC) hybrid KeyShare processing. In the error handling path of TLSX_KeyShare_ProcessPqcHybridClient() in src/tls.c, the inner function TLSX_KeyShare_ProcessPqcClient_ex() frees a KyberKey object upon encountering an error. The caller then invokes TLSX_KeyShare_FreeAll(), which attempts to call ForceZero() on the already-freed KyberKey, resulting in writes of zero bytes over freed heap memory.	N/A	More Details
CVE-2026-34942	Wasmtime is a runtime for WebAssembly. Prior to 24.0.7, 36.0.7, 42.0.2, and 43.0.1, Wasmtime's implementation of transcoding strings into the Component Model's utf16 or latin1+utf16 encodings improperly verified the alignment of reallocated strings. This meant that unaligned pointers could be passed to the host for transcoding which would trigger a host panic. This panic is possible to trigger from malicious guests which transfer very specific strings across components with specific addresses. Host panics are considered a DoS vector in Wasmtime as the panic conditions	N/A	More Details

	are controlled by the guest in this situation. This vulnerability is fixed in 24.0.7, 36.0.7, 42.0.2, and 43.0.1.		
CVE-2025-14551	In Ubuntu, Subiquity version 24.04.4 could leak sensitive user credentials during crash reporting. Upon installation failure, if a user submitted a bug report to Launchpad, Subiquity could include certain user credentials, such as the user's plaintext Wi-Fi password, in the attached logs.	N/A	More Details
CVE-2025-15480	In Ubuntu, ubuntu-desktop-provision version 24.04.4 could leak sensitive user credentials during crash reporting. Upon installation failure, if a user submitted a bug report to Launchpad, ubuntu-desktop-provision could include the user's password hash in the attached logs.	N/A	More Details
CVE-2026-35204	Helm is a package manager for Charts for Kubernetes. From 4.0.0 to 4.1.3, a specially crafted Helm plugin, when installed or updated, will cause Helm to write the contents of the plugin to an arbitrary filesystem location. To prevent this, validate that the plugin.yaml of the Helm plugin does not include a version: field containing POSIX dot-dot path separators ie. "/../". This vulnerability is fixed in 4.1.4.	N/A	More Details
CVE-2026-5448	X.509 date buffer overflow in wolfSSL_X509_notAfter / wolfSSL_X509_notBefore. A buffer overflow may occur when parsing date fields from a crafted X.509 certificate via the compatibility layer API. This is only triggered when calling these two APIs directly from an application, and does not affect TLS or certificate verify operations in wolfSSL.	N/A	More Details
CVE-2026-5393	Dual-Algorithm CertificateVerify out-of-bounds read. When processing a dual-algorithm CertificateVerify message, an out-of-bounds read can occur on crafted input. This can only occur when --enable-experimental and --enable-dual-alg-certs is used when building wolfSSL.	N/A	More Details
CVE-2026-5392	Heap out-of-bounds read in PKCS7 parsing. A crafted PKCS7 message can trigger an OOB read on the heap. The missing bounds check is in the indefinite-length end-of-content verification loop in PKCS7_VerifySignedData().	N/A	More Details
CVE-2026-35205	Helm is a package manager for Charts for Kubernetes. From 4.0.0 to 4.1.3, Helm will install plugins missing provenance (.prov file) when signature verification is required. This vulnerability is fixed in 4.1.4.	N/A	More Details
CVE-2026-5507	When restoring a session from cache, a pointer from the serialized session data is used in a free operation without validation. An attacker who can poison the session cache could trigger an arbitrary free. Exploitation requires the ability to inject a crafted session into the cache and for the application to call specific session restore APIs.	N/A	More Details
CVE-2026-5504	A padding oracle exists in wolfSSL's PKCS7 CBC decryption that could allow an attacker to recover plaintext through repeated decryption queries with modified ciphertext. In previous versions of wolfSSL the interior padding bytes are not validated.	N/A	More Details
CVE-2026-5503	In TLSX_EchChangeSNI, the ctx->extensions branch set extensions unconditionally even when TLSX_Find returned NULL. This caused TLSX_UseSNI to attach the attacker-controlled publicName to the shared WOLFSSL_CTX when no inner SNI was configured. TLSX_EchRestoreSNI then failed to clean it up because its removal was gated on serverNameX != NULL. The inner ClientHello was sized before the pollution but written after it, causing TLSX_SNI_Write to memcpy 255 bytes past the allocation boundary.	N/A	More Details
CVE-2026-5295	A stack buffer overflow exists in wolfSSL's PKCS7 implementation in the wc_PKCS7_DecryptOri() function in wolfcrypt/src/pkcs7.c. When processing a CMS EnvelopedData message containing an OtherRecipientInfo (ORI) recipient, the function copies an ASN.1-parsed OID into a fixed 32-byte stack buffer (oriOID[MAX_OID_SZ]) via XMEMCPY without first validating that the parsed OID length does not exceed MAX_OID_SZ. A crafted CMS EnvelopedData message with an ORI recipient containing an OID longer than 32 bytes triggers a stack buffer overflow. Exploitation requires the library to be built with --enable-pkcs7 (disabled by default) and the application to have registered an ORI decrypt callback via wc_PKCS7_SetOriDecryptCb().	N/A	More Details
CVE-2026-5778	Integer underflow in wolfSSL packet sniffer <= 5.9.0 allows an attacker to cause a program crash in the AEAD decryption path by injecting a TLS record shorter than the explicit IV plus authentication tag into traffic inspected by ssl_DecodePacket. The underflow wraps a 16-bit length to a large value that is passed to AEAD decryption routines, causing a large out-of-bounds read and crash. An unauthenticated attacker can trigger this remotely via malformed TLS Application Data records.	N/A	More Details
CVE-2026-5772	A 1-byte stack buffer over-read was identified in the MatchDomainName function (src/internal.c) during wildcard hostname validation when the LEFT_MOST_WILDCARD_ONLY flag is active. If a wildcard * exhausts the entire hostname string, the function reads one byte past the buffer without a bounds check, which could cause a crash.	N/A	More Details
CVE-2026-5264	Heap buffer overflow in DTLS 1.3 ACK message processing. A remote attacker can send a crafted DTLS 1.3 ACK message that triggers a heap buffer overflow.	N/A	More Details
CVE-2026-5263	URI nameConstraints from constrained intermediate CAs are parsed but not enforced during certificate chain verification in wolfcrypt/src/asn.c. A compromised or malicious sub-CA could issue leaf certificates with URI SAN entries that violate the nameConstraints of the issuing CA, and wolfSSL would accept them as valid.	N/A	More Details
CVE-2026-5883	Use after free in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, he memory hooks executor in praisonaiagents passes a user-controlled command string directly to subprocess.run() with shell=True at src/praisonai-agents/praisonaiagents/memory/hooks.py. No sanitization is performed and shell metacharacters are interpreted by		

CVE-2026-40111	/bin/sh before the intended command executes. Two independent attack surfaces exist. The first is via pre_run_command and post_run_command hook event types registered through the hooks configuration. The second and more severe surface is the .praisonai/hooks.json lifecycle configuration, where hooks registered for events such as BEFORE_TOOL and AFTER_TOOL fire automatically during agent operation. An agent that gains file-write access through prompt injection can overwrite .praisonai/hooks.json and have its payload execute silently at every subsequent lifecycle event without further user interaction. This vulnerability is fixed in 1.5.128.	N/A	More Details
CVE-2026-5754	Reflected Cross-Site Scripting (XSS) Vulnerability in Radware Alteon 34.5.4.0 vADC load-balancer allows an attacker to inject malicious scripts into the website, potentially leading to unauthorized actions, data theft, or other malicious activities.	N/A	More Details
CVE-2026-5756	Unauthenticated Configuration File Modification Vulnerability in DRC Central Office Services (COS) allows an attacker to modify the server's configuration file, potentially leading to mass data exfiltration, malicious traffic interception, or disruption of testing services.	N/A	More Details
CVE-2026-5890	Race in WebCodecs in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2026-1502	CR/LF bytes were not rejected by HTTP client proxy tunnel headers or host.	N/A	More Details
CVE-2026-39398	Rejected reason: The affected product and advisory are not public.	N/A	More Details
CVE-2026-5447	Heap buffer overflow in CertFromX509 via AuthorityKeyIdentifier size confusion. A heap buffer overflow occurs when converting an X.509 certificate internally due to incorrect size handling of the AuthorityKeyIdentifier extension.	N/A	More Details
CVE-2026-5446	In wolfSSL, ARIA-GCM cipher suites used in TLS 1.2 and DTLS 1.2 reuse an identical 12-byte GCM nonce for every application-data record. Because wc_AriaEncrypt is stateless and passes the caller-supplied IV verbatim to the MagicCrypto SDK with no internal counter, and because the explicit IV is zero-initialized at session setup and never incremented in non-FIPS builds. This vulnerability affects wolfSSL builds configured with --enable-aria and the proprietary MagicCrypto SDK (a non-default, opt-in configuration required for Korean regulatory deployments). AES-GCM is not affected because wc_AesGcmEncrypt_ex maintains an internal invocation counter independently of the call-site guard.	N/A	More Details
CVE-2026-39957	Lychee is a free, open-source photo-management tool. Prior to 7.5.4, a SQL operator-precedence bug in SharingController::listAll() causes the orWhereNotNull('user_group_id') clause to escape the ownership filter applied by the when() block. Any authenticated non-admin user with upload permission who owns at least one album can retrieve all user-group-based sharing permissions across the entire instance, including private albums owned by other users. This vulnerability is fixed in 7.5.4.	N/A	More Details
CVE-2025-13822	MCPHub in versions below 0.11.0 is vulnerable to authentication bypass. Some endpoints are not protected by authentication middleware, allowing an unauthenticated attacker to perform actions in the name of other users and using their privileges.	N/A	More Details
CVE-2026-4157	ChargePoint Home Flex revssh Service Command Injection Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of ChargePoint Home Flex devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of OCPP messages. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-26338.	N/A	More Details
CVE-2026-33698	Chamilo LMS is a learning management system. Prior to 1.11.38, a chained attack can enable otherwise-blocked PHP code from the main/install/ directory and allow an unauthenticated attacker to modify existing files or create new files where allowed by system permissions. This only affects portals with the main/install/ directory still present and read-accessible. This vulnerability is fixed in 1.11.38.	N/A	More Details
CVE-2026-34188	Improper Neutralization of Special Elements used in an OS Command vulnerability allows OS Command Injection via Event Response execution. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-2400	CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability exists that could cause application user credentials to reset when a Web Admin user alters the POST /setPCBEDesc request payload.	N/A	More Details
CVE-2026-2401	CWE-532 Insertion of Sensitive Information into Log File vulnerability exists that could cause confidential information to be exposed when a Web Admin user executes a malicious file provided by an attacker.	N/A	More Details
CVE-2026-2402	CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that would allow an attacker to gain access to the user account by performing an arbitrary number of authentication attempts with different credentials on a sequence of requests to multiple endpoints.	N/A	More Details

CVE-2026-2403	CWE-1284 Improper Validation of Specified Quantity in Input vulnerability exists that could cause Event and Data Log truncation impacting log integrity when a Web Admin user alters the POST /logsettings request payload.	N/A	More Details
CVE-2026-2404	CWE-116 Improper Encoding or Escaping of Output vulnerability exists that could cause log injection and forged log when an attacker alters the POST /j_security check request payload.	N/A	More Details
CVE-2026-2405	CWE-400 Uncontrolled Resource Consumption vulnerability exists that could cause excessive troubleshooting zip file creation and denial of service when a Web Admin user floods the system with POST /helpabout requests.	N/A	More Details
CVE-2026-39686	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in bannersky BSK PDF Manager bsk-pdf-manager allows Retrieve Embedded Sensitive Data.This issue affects BSK PDF Manager: from n/a through <= 3.7.2.	N/A	More Details
CVE-2026-6100	Use-after-free (UAF) was possible in the `lzma.LZMADecompressor`, `bz2.BZ2Decompressor`, and `gzip.GzipFile` when a memory allocation fails with a `MemoryError` and the decompression instance is re-used. This scenario can be triggered if the process is under memory pressure. The fix cleans up the dangling pointer in this specific error condition. The vulnerability is only present if the program re-uses decompressor instances across multiple decompression calls even after a `MemoryError` is raised during decompression. Using the helper functions to one-shot decompress data such as `lzma.decompress()`, `bz2.decompress()`, `gzip.decompress()`, and `zlib.decompress()` are not affected as a new decompressor instance is used per call. If the decompressor instance is not re-used after an error condition, this usage is similarly not vulnerable.	N/A	More Details
CVE-2026-39689	Missing Authorization vulnerability in eshipper eShipper Commerce eshipper-commerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects eShipper Commerce: from n/a through <= 2.16.12.	N/A	More Details
CVE-2026-39940	ChurchCRM is an open-source church management system. Prior to 7.0.0, it was possible in many places across the ChurchCRM application to create a link that, when visited by an authenticated user, would redirect them to any URL chosen by an attacker if they clicked 'Cancel' button on the page. For this write-up the DonatedItemEditor.php will be used as an example, however wherever all instances of 'linkBack' should be assessed. This vulnerability is fixed in 7.0.0.	N/A	More Details
CVE-2026-38533	An improper authorization vulnerability in the /api/v1/users/{id} endpoint of Snipe-IT v8.4.0 allows authenticated attackers with the users.edit permission to modify sensitive authentication and account-state fields of other non-admin users via supplying a crafted PUT request.	N/A	More Details
CVE-2026-23891	Decidim is a participatory democracy framework. In versions below 0.30.5 and 0.31.0.rc1 through 0.31.0, a stored code execution vulnerability in the user name field allows a low-privileged attacker to execute arbitrary code in the context of any user who passively visits a comment page, resulting in high confidentiality and integrity impact across security boundaries. This issue has been fixed in versions 0.30.5 and 0.31.1.	N/A	More Details
CVE-2026-4832	CWE-798 Use of Hard-coded Credentials vulnerability exists that could cause unauthorized access to sensitive device information when an unauthenticated attacker is able to interrogate the SNMP port.	N/A	More Details
CVE-2026-5713	The "profiling.sampling" module (Python 3.15+) and "asyncio introspection capabilities" (3.14+, "python -m asyncio ps" and "python -m asyncio pstree") features could be used to read and write addresses in a privileged process if that process connected to a malicious or "infected" Python process via the remote debugging feature. This vulnerability requires persistently and repeatedly connecting to the process to be exploited, even after the connecting process crashes with high likelihood due to ASLR.	N/A	More Details
CVE-2026-34186	Improper Neutralization of Special Elements used in an SQL Command vulnerability allows SQL Injection via custom fields. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-31426	In the Linux kernel, the following vulnerability has been resolved: ACPI: EC: clean up handlers on probe failure in acpi_ec_setup() When ec_install_handlers() returns -EPROBE_DEFER on reduced-hardware platforms, it has already started the EC and installed the address space handler with the struct acpi_ec pointer as handler context. However, acpi_ec_setup() propagates the error without any cleanup. The caller acpi_ec_add() then frees the struct acpi_ec for non-boot instances, leaving a dangling handler context in ACPICA. Any subsequent AML evaluation that accesses an EC OpRegion field dispatches into acpi_ec_space_handler() with the freed pointer, causing a use-after-free: BUG: KASAN: slab-use-after-free in mutex_lock (kernel/locking/mutex.c:289) Write of size 8 at addr ffff88800721de38 by task init/1 Call Trace: <TASK> mutex_lock (kernel/locking/mutex.c:289) acpi_ec_space_handler (drivers/acpi/ec.c:1362) acpi_ev_address_space_dispatch (drivers/acpi/acpica/evregion.c:293) acpi_ex_access_region (drivers/acpi/acpica/exfldio.c:246) acpi_ex_field_datum_io (drivers/acpi/acpica/exfldio.c:509) acpi_ex_extract_from_field (drivers/acpi/acpica/exfldio.c:700) acpi_ex_read_data_from_field (drivers/acpi/acpica/exfield.c:327) acpi_ex_resolve_node_to_value (drivers/acpi/acpica/exresolv.c:392) </TASK> Allocated by task 1: acpi_ec_alloc (drivers/acpi/ec.c:1424) acpi_ec_add (drivers/acpi/ec.c:1692) Freed by task 1: kfree (mm/slub.c:6876) acpi_ec_add (drivers/acpi/ec.c:1751) The bug triggers on reduced-hardware EC platforms (ec->gpe < 0) when the GPIO IRQ provider defers probing. Once the stale handler exists, any unprivileged sysfs read that causes AML to touch an EC OpRegion (battery, thermal, backlight) exercises the dangling pointer. Fix this by calling ec_remove_handlers() in the error path of acpi_ec_setup() before clearing first_ec. ec_remove_handlers() checks each EC_FLAGS_* bit before acting, so it is safe to call regardless of how far ec_install_handlers() progressed: -ENODEV	N/A	More Details

	(handler not installed): only calls acpi_ec_stop() -EPROBE_DEFER (handler installed): removes handler, stops EC		
CVE-2026-30813	Improper Neutralization of Special Elements used in an SQL Command vulnerability allows SQL Injection via module search. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-30812	Improper Neutralization of Input During Web Page Generation vulnerability allows Stored Cross-Site Scripting via event comments. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-30811	Missing Authorization vulnerability allows Exposure of Sensitive Information via configuration endpoint. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-30809	Improper Neutralization of Special Elements used in an OS Command vulnerability allows OS Command Injection via WebServerModuleDebug. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-30806	Improper Neutralization of Special Elements used in an OS Command vulnerability allows OS Command Injection via Network Report. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2026-30804	Unrestricted Upload of File with Dangerous Type vulnerability allows Remote Code Execution via file upload. This issue affects Pandora FMS: from 777 through 800	N/A	More Details
CVE-2025-70023	An issue pertaining to CWE-843: Access of Resource Using Incompatible Type was discovered in transloadit uppy v0.25.6.	N/A	More Details
CVE-2026-0207	A vulnerability exists in FlashBlade whereby sensitive information may be logged under specific conditions.	N/A	More Details
CVE-2026-0209	Under certain administrative conditions, FlashArray Purity may apply snapshot retention policies earlier or later than configured.	N/A	More Details
CVE-2026-1462	A vulnerability in the `TFSMLayer` class of the `keras` package, version 3.13.0, allows attacker-controlled TensorFlow SavedModels to be loaded during deserialization of `.keras` models, even when `safe_mode=True`. This bypasses the security guarantees of `safe_mode` and enables arbitrary attacker-controlled code execution during model inference under the victim's privileges. The issue arises due to the unconditional loading of external SavedModels, serialization of attacker-controlled file paths, and the lack of validation in the `from_config()` method.	N/A	More Details
CVE-2025-66236	Before Airflow 3.2.0, it was unclear that secure Airflow deployments require the Deployment Manager to take appropriate actions and pay attention to security details and security model of Airflow. Some assumptions the Deployment Manager could make were not clear or explicit enough, even though Airflow's intentions and security model of Airflow did not suggest different assumptions. The overall security model [1], workload isolation [2], and JWT authentication details [3] are now described in more detail. Users concerned with role isolation and following the Airflow security model of Airflow are advised to upgrade to Airflow 3.2, where several security improvements have been implemented. They should also read and follow the relevant documents to make sure that their deployment is secure enough. It also clarifies that the Deployment Manager is ultimately responsible for securing your Airflow deployment. This had also been communicated via Airflow 3.2.0 Blog announcement [4]. [1] Security Model: https://airflow.apache.org/docs/apache-airflow/stable/security/jwt_token_authentication.html [2] Workload isolation: https://airflow.apache.org/docs/apache-airflow/stable/security/workload.html [3] JWT Token authentication: https://airflow.apache.org/docs/apache-airflow/stable/security/jwt_token_authentication.html [4] Airflow 3.2.0 Blog announcement: https://airflow.apache.org/blog/airflow-3.2.0/ Users are recommended to upgrade to version 3.2.0, which fixes this issue.	N/A	More Details
CVE-2026-31428	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_log: fix uninitialized padding leak in NFULA_PAYLOAD __build_packet_message() manually constructs the NFULA_PAYLOAD netlink attribute using skb_put() and skb_copy_bits(), bypassing the standard nla_reserve()/nla_put() helpers. While nla_total_size(data_len) bytes are allocated (including NLA alignment padding), only data_len bytes of actual packet data are copied. The trailing nla_padlen(data_len) bytes (1-3 when data_len is not 4-byte aligned) are never initialized, leaking stale heap contents to userspace via the NFLOG netlink socket. Replace the manual attribute construction with nla_reserve(), which handles the tailroom check, header setup, and padding zeroing via __nla_reserve(). The subsequent skb_copy_bits() fills in the payload data on top of the properly initialized attribute.	N/A	More Details
CVE-2026-31427	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_sip: fix use of uninitialized rtp_addr in process_sdp process_sdp() declares union nf_inet_addr rtp_addr on the stack and passes it to the nf_nat_sip sdp_session hook after walking the SDP media descriptions. However rtp_addr is only initialized inside the media loop when a recognized media type with a non-zero port is found. If the SDP body contains no m= lines, only inactive media sections (m=audio 0 ...) or only unrecognized media types, rtp_addr is never assigned. Despite that, the function still calls hooks->sdp_session() with &rtp_addr, causing nf_nat_sdp_session() to format the stale stack value as an IP address and rewrite the SDP session owner and connection lines with it. With CONFIG_INIT_STACK_ALL_ZERO (default on most distributions) this results in the session-level o= and c= addresses	N/A	More Details

	being rewritten to 0.0.0.0 for inactive SDP sessions. Without stack auto-init the rewritten address is whatever happened to be on the stack. Fix this by pre-initializing rtp_addr from the session-level connection address (caddr) when available, and tracking via a have_rtp_addr flag whether any valid address was established. Skip the sdp_session hook entirely when no valid address exists.		
CVE-2026-24906	October is a Content Management System (CMS) and web platform. Versions prior to 3.7.14 and 4.1.10 contain a Stored Cross-Site Scripting (XSS) vulnerability in the Backend Editor Settings. The Markup Classes fields (used for paragraph styles, inline styles, table styles, etc.) did not sanitize input to valid CSS class name characters. Malicious values were rendered unsanitized in Froala editor dropdown menus, allowing JavaScript execution when any user opened a RichEditor. Exploitation could lead to privilege escalation if a superuser opens any RichEditor during routine content editing (e.g., editing a blog post), and requires authenticated backend access with editor settings permissions. This issue has been fixed in versions 3.7.14 and 4.1.10. To workaround this issue, restrict editor settings permissions to fully trusted administrators only	N/A	More Details
CVE-2026-2399	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause critical files overwritten with text data when a Web Admin user alters the POST /REST/upssleep request payload.	N/A	More Details
CVE-2026-29955	The `/registercrd` endpoint in KubePlus 4.14 in the kubeconfiggenerator component is vulnerable to command injection. The component uses `subprocess.Popen()` with `shell=True` parameter to execute shell commands, and the user-supplied `chartName` parameter is directly concatenated into the command string without any sanitization or validation. An attacker can inject arbitrary shell commands by crafting a malicious `chartName` parameter value.	N/A	More Details
CVE-2026-31048	An issue in the <code>pickle</code> protocol of Pyro v3.x allows attackers to execute arbitrary code via supplying a crafted pickled string message.	N/A	More Details
CVE-2026-39654	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ashish Ajani WP Simple HTML Sitemap wp-simple-html-sitemap allows DOM-Based XSS.This issue affects WP Simple HTML Sitemap: from n/a through <= 3.8.	N/A	More Details
CVE-2026-2449	Improper neutralization of argument delimiters in a command ('argument injection') vulnerability in upKeeper Solutions upKeeper Instant Privilege Access allows Hijacking a Privileged Thread of Execution.This issue affects upKeeper Instant Privilege Access: through 1.5.0.	N/A	More Details
CVE-2024-9168	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-2450	.NET misconfiguration: use of impersonation vulnerability in upKeeper Solutions upKeeper Instant Privilege Access allows Hijacking a Privileged Thread of Execution.This issue affects upKeeper Instant Privilege Access: through 1.5.0.	N/A	More Details
CVE-2026-5307	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-7389	A vulnerability in the AdminServer component of OpenEdge on all supported platforms grants its authenticated users OS-level access to the server through the adopted authority of the AdminServer process itself. The delegated authority of the AdminServer could allow its users the ability to read arbitrary files on the host system through the misuse of the setFile() and openFile() methods exposed through the RMI interface. Misuse was limited only by OS-level authority of the AdminServer's elevated privileges granted and the user's access to these methods enabled through RMI. The exploitable methods have been removed thus eliminating their access through RMI or downstream of the RMI registry.	N/A	More Details
CVE-2025-8095	The OECH1 prefix encoding is intended to obfuscate values across the OpenEdge platform. It has been identified as cryptographically weak and unsuitable for stored encodings and enterprise applications. OECH1 encodings should be considered exploitable and immediately replaced by any other supported prefix encoding, all of which are based on symmetric encryption.	N/A	More Details
CVE-2026-31049	An issue in Hostbill v.2025-11-24 and 2025-12-01 allows a remote attacker to execute arbitrary code and escalate privileges via the CSV registration field	N/A	More Details
CVE-2025-61260	A vulnerability was identified in OpenAI Codex CLI v0.23.0 and before that enables code execution through malicious MCP (Model Context Protocol) configuration files. The attack is triggered when a user runs the codex command inside a malicious or compromised repository. Codex automatically loads project-local .env and .codex/config.toml files without requiring user confirmation, allowing attackers to embed arbitrary commands that execute immediately.	N/A	More Details
CVE-2025-69893	A side-channel vulnerability exists in the implementation of BIP-39 mnemonic processing, as observed in Trezor One v1.13.0 to v1.14.0, Trezor T v1.13.0 to v1.14.0, and Trezor Safe v1.13.0 to v1.14.0 hardware wallets. This originates from the BIP-39 standard guidelines, which induce non-constant time execution and specific branch patterns for word searching. An attacker with physical access during the initial setup phase can collect a single side-channel trace. By utilizing profiling-based Deep Learning Side-Channel Analysis (DL-SCA), the attacker can recover the mnemonic code and subsequently steal the assets. The issue was patched.	N/A	More Details
CVE-	A Local File Inclusion (LFI) vulnerability in the NFSen module (nfsen.inc.php) of LibreNMS 22.11.0-23-gd091788f2		

2026-30480	allows authenticated attackers to include arbitrary PHP files from the server filesystem via path traversal sequences in the nfsen parameter.	N/A	More Details
CVE-2026-40315	PraisonAI is a multi-agent teams system. Prior to 4.5.133, there is an SQL identifier injection vulnerability in SQLiteConversationStore where the table_prefix configuration value is directly concatenated into SQL queries via f-strings without any validation or sanitization. Since SQL identifiers cannot be safely parameterized, an attacker who controls the table_prefix value (e.g., through from_yaml or from_dict configuration input) can inject arbitrary SQL fragments that alter query structure. This enables unauthorized data access, such as reading internal SQLite tables like sqlite_master, and manipulation of query results through techniques like UNION-based injection. The vulnerability propagates from configuration input in config.py, through factory.py, to the SQL query construction in sqlite.py. Exploitation requires the ability to influence configuration input, and successful exploitation leads to internal schema disclosure and full query result tampering. This issue has been fixed in version 4.5.133.	N/A	More Details
CVE-2026-34984	External Secrets Operator reads information from a third-party service and automatically injects the values as Kubernetes Secrets. Versions 2.2.0 and below contain a vulnerability in runtime/template/v2/template.go where the v2 template engine removes env and expandenv from Sprig's TxtFuncMap() but leaves the getHostByName function accessible to user-controlled templates. Since ESO executes templates within the controller process, an attacker who can create or update templated ExternalSecret resources can invoke controller-side DNS lookups using secret-derived values. This creates a DNS exfiltration primitive, allowing fetched secret material to be leaked via DNS queries without requiring direct outbound network access from the attacker's workload. The impact is a confidentiality issue, particularly in environments where untrusted or lower-trust users can author templated ExternalSecret resources and the controller has DNS resolution capability. This issue has been fixed in version 2.3.0.	N/A	More Details
CVE-2026-39426	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain a Stored Cross-Site Scripting (XSS) vulnerability where the frontend's MdRenderer.vue component parses custom <iframe_render> tags from LLM responses or Application Prologue configurations, bypassing standard Markdown sanitization and XSS filtering. The unsanitized HTML content is passed to the IframeRender.vue component, which renders it directly into an <iframe> via the srcdoc attribute configured with sandbox="allow-scripts allow-same-origin". This can be a dangerous combination, allowing injected scripts to escape the iframe and execute JavaScript in the parent window using window.parent. Since the Prologue is rendered for any user visiting an application's chat interface, this results in a high-impact Stored XSS that can lead to session hijacking, unauthorized actions, and sensitive data exposure. This issue has been fixed in version 2.8.0.	N/A	More Details
CVE-2026-39425	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain a Stored Cross-Site Scripting (XSS) vulnerability that allows authenticated users to inject arbitrary HTML and JavaScript into the Application prologue (Opening Remarks) field by wrapping malicious payloads in <html_rander> tags. The backend fails to sanitize or encode HTML entities in the prologue field when applications are created or updated via the /admin/api/workspace/{workspace_id}/application endpoint, storing the raw payload directly in the database. The frontend then renders this content using an innerHTML-equivalent mechanism, trusting <html_rander>-wrapped content to be safe, which enables persistent DOM-based Stored XSS execution against any visitor who opens the affected chatbot interface. Exploitation can lead to session hijacking, unauthorized actions performed on behalf of victims (such as deleting workspaces or applications), and sensitive data exposure. This issue has been fixed in version 2.8.0.	N/A	More Details
CVE-2026-39424	MaxKB is an open-source AI assistant for enterprise. In versions 2.7.1 and below, the chat export feature is vulnerable to Improper Neutralization of Formula Elements in a CSV File. When an administrator exports the application chat history to an Excel file (.xlsx) via the /admin/api/workspace/{workspace_id}/application/{application_id}/chat/export endpoint, strings starting with formula characters are written directly without proper sanitization. Opening this file in spreadsheet applications like Microsoft Excel can lead to Arbitrary Code Execution (RCE) on the administrator's workstation via Dynamic Data Exchange (DDE). The issue is a variant of CVE-2025-4546, which fixed the exact same pattern in apps/dataset/serializers/document_serializers.py but missed the application chat export sink. This issue has been fixed in version 2.8.0.	N/A	More Details
CVE-2026-39423	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain an Eval Injection vulnerability in the Markdown rendering engine that allows any user capable of interacting with the AI chat interface to execute arbitrary JavaScript in the browsers of other users, including administrators, resulting in Stored Cross-Site Scripting (XSS). This issue has been fixed in version 2.8.0.	N/A	More Details
CVE-2026-39422	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain a Stored Cross-Site Scripting (XSS) vulnerability through the application name or icon fields when creating an application. When a victim visits the public chat interface (/ui/chat/{access_token}), the ChatHeadersMiddleware retrieves the application data and directly inserts the unescaped application name and icon into the HTML response via string replacement. This allows an attacker to execute arbitrary JavaScript in the victim's browser context. This issue has been fixed in version 2.8.0.	N/A	More Details
CVE-2026-33948	jq is a command-line JSON processor. Commits before 6374ae0bcdfe33a18eb0ae6db28493b1f34a0a5b contain a vulnerability where CLI input parsing allows validation bypass via embedded NUL bytes. When reading JSON from files or stdin, jq uses strlen() to determine buffer length instead of the actual byte count from fgets(), causing it to truncate input at the first NUL byte and parse only the preceding prefix. This enables an attacker to craft input with a benign JSON prefix before a NUL byte followed by malicious trailing data, where jq validates only the prefix as valid JSON while silently discarding the suffix. Workflows relying on jq to validate untrusted JSON before forwarding it to downstream consumers are susceptible to parser differential attacks, as those consumers may process the full input including the malicious trailing bytes. This issue has been patched by commit 6374ae0bcdfe33a18eb0ae6db28493b1f34a0a5b.	N/A	More Details
CVE-	Crypt::SecretBuffer versions before 0.019 for Perl is suseceptible to timing attacks. For example, if Crypt::SecretBuffer		More

2026-5086	was used to store and compare plaintext passwords, then discrepencies in timing could be used to guess the secret password.	N/A	Details
CVE-2026-39979	jq is a command-line JSON processor. In commits before 2f09060afab23fe9390cce7cb860b10416e1bf5f, the jv_parse_sized() API in libjq accepts a counted buffer with an explicit length parameter, but its error-handling path formats the input buffer using %s in jv_string_fmt(), which reads until a NUL terminator is found rather than respecting the caller-supplied length. This means that when malformed JSON is passed in a non-NUL-terminated buffer, the error construction logic performs an out-of-bounds read past the end of the buffer. The vulnerability is reachable by any libjq consumer calling jv_parse_sized() with untrusted input, and depending on memory layout, can result in memory disclosure or process termination. The issue has been patched in commit 2f09060afab23fe9390cce7cb860b10416e1bf5f.	N/A	More Details
CVE-2026-4786	Mitgation of CVE-2026-4519 was incomplete. If the URL contained "%action" the mitigation could be bypassed for certain browser types the "webbrowser.open()" API could have commands injected into the underlying shell. See CVE-2026-4519 for details.	N/A	More Details
CVE-2025-65133	A SQL injection vulnerability exists in the School Management System (version 1.0) by manikandan580. An unauthenticated or authenticated remote attacker can supply a crafted HTTP request to the affected endpoint to manipulate SQL query logic and extract sensitive database information.	N/A	More Details
CVE-2025-65134	In manikandan580 School-management-system 1.0, a reflected cross-site scripting (XSS) vulnerability exists in /studentms/admin/contact-us.php via the email POST parameter.	N/A	More Details
CVE-2026-32272	Craft Commerce is an ecommerce platform for Craft CMS. In versions 5.0.0 through 5.5.4, an SQL injection vulnerability exists where the ProductQuery::hasVariant and VariantQuery::hasProduct properties bypass the input sanitization blocklist added to ElementIndexesController in a prior security fix (GHSA-2453-mppf-46cj). The blocklist only strips top-level Yii2 Query properties such as where and orderBy, but hasVariant and hasProduct pass through untouched and internally call Craft::configure() on a subquery without sanitization, re-introducing SQL injection. Any authenticated control panel user can exploit this via boolean-based blind SQL injection to extract arbitrary database contents, including security keys that enable forging admin sessions for privilege escalation. This issue has been fixed in version 5.6.0.	N/A	More Details
CVE-2026-32271	Craft Commerce is an ecommerce platform for Craft CMS. In versions 4.0.0 through 4.10.2 and 5.0.0 through 5.5.4, there is an SQL injection vulnerability in the Commerce TotalRevenue widget which allows any authenticated control panel user to achieve remote code execution through a four-step exploitation chain. The attack exploits unsanitized widget settings interpolated into SQL expressions, combined with PDO's default multi-statement query support, to inject a maliciously serialized PHP object into the queue table. When the queue consumer processes the injected job, the unrestricted unserialize() call in yii2-queue instantiates a GuzzleHttp FileCookieJar gadget chain whose __destruct() method writes a PHP webshell to the server's webroot. The complete chain requires only three HTTP requests, no administrative privileges, and results in arbitrary command execution as the PHP process user, with queue processing triggered via an unauthenticated endpoint. This issue has been fixed in versions 4.10.3 and 5.5.5.	N/A	More Details
CVE-2026-31280	An issue in the Bluetooth RFCOMM service of Parani M10 Motorcycle Intercom v2.1.3 allows unauthorized attackers to cause a Denial of Service (DoS) via supplying crafted RFCOMM frames.	N/A	More Details
CVE-2026-26460	A HTML Injection vulnerability exists in the Dashboard module of Vtiger CRM 8.4.0. The application fails to properly neutralize user-supplied input in the tabid parameter of the DashBoardTab view (getTabContents action), allowing an attacker to inject arbitrary HTML content into the dashboard interface. The injected content is rendered in the victim's browser	N/A	More Details
CVE-2025-51414	In Phpgurukul Online Course Registration v3.1, an arbitrary file upload vulnerability was discovered within the profile picture upload functionality on the /my-profile.php page.	N/A	More Details
CVE-2026-32270	Craft Commerce is an ecommerce platform for Craft CMS. In versions 4.0.0 through 4.10.2 and 5.0.0 through 5.5.4, the PaymentsController::actionPay discloses some order data to unauthenticated users when an order number is provided and the email check fails during an anonymous payment. The JSON error response includes the serialized order object (order), which contains some sensitive fields such as customer email, shipping address, and billing address. The frontend payment flow's actionPay() retrieves orders by number before authorization is fully enforcedLoad order by number. This issue has been fixed in versions 4.11.0 and 5.6.0.	N/A	More Details
CVE-2026-24907	October is a Content Management System (CMS) and web platform. Versions prior to 3.7.14 and 4.1.10 contain a stored cross-site scripting (XSS) vulnerability in the Event Log mail preview feature. When viewing logged mail messages, HTML content was rendered in an iframe without proper sandboxing, allowing JavaScript execution in the viewer's browser context. This issue has been fixed in versions 3.7.14 and 4.1.10. If users are unable to update immediately, workarounds include restricting mail template editing permissions to fully trusted administrators only and restricting Event Log viewing permissions to minimize exposure.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: rds: ib: reject FRMR registration before IB connection is established rds_ib_get_mr() extracts the rds_ib_connection from conn->c_transport_data and passes it to rds_ib_reg_frmr() for FRWR memory registration. On a fresh outgoing connection, ic is allocated in rds_ib_conn_alloc() with i_cm_id = NULL because the connection worker has not yet called rds_ib_conn_path_connect() to create the rdma_cm_id. When sendmsg() with RDS_CMSG_RDMA_MAP is called on such a connection, the sendmsg path parses the control message before any connection establishment, allowing		

CVE-2026-31425	rds_ib_post_reg_frmr() to dereference ic->i_cm_id->qp and crash the kernel. The existing guard in rds_ib_reg_frmr() only checks for !ic (added in commit 9e630bcb7701), which does not catch this case since ic is allocated early and is always non-NULL once the connection object exists. KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] RIP: 0010:rds_ib_post_reg_frmr+0x50e/0x920 Call Trace: rds_ib_post_reg_frmr (net/rds/ib_frmr.c:167) rds_ib_map_frmr (net/rds/ib_frmr.c:252) rds_ib_reg_frmr (net/rds/ib_frmr.c:430) rds_ib_get_mr (net/rds/ib_rdma.c:615) __rds_rdma_map (net/rds/rdma.c:295) rds_cmsg_rdma_map (net/rds/rdma.c:860) rds_sendmsg (net/rds/send.c:1363) ____sys_sendmsg do_syscall_64 Add a check in rds_ib_get_mr() that verifies ic, i_cm_id, and qp are all non-NULL before proceeding with FRMR registration, mirroring the guard already present in rds_ib_post_inv(). Return -ENODEV when the connection is not ready, which the existing error handling in rds_cmsg_send() converts to -EAGAIN for userspace retry and triggers rds_conn_connect_if_down() to start the connection worker.	N/A	More Details
CVE-2026-33703	Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the /social-network/personal-data/{userId} endpoint allows any authenticated user to access full personal data and API tokens of arbitrary users by modifying the userId parameter. This results in mass disclosure of sensitive user information and credentials, enabling a full platform data breach. This vulnerability is fixed in 2.0.0-RC.3.	N/A	More Details
CVE-2026-4152	GIMP JP2 File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28863.	N/A	More Details
CVE-2026-5495	Labcenter Electronics Proteus PDSPRJ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Labcenter Electronics Proteus. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of PDSPRJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25720.	N/A	More Details
CVE-2026-5494	Labcenter Electronics Proteus PDSPRJ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Labcenter Electronics Proteus. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of PDSPRJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25719.	N/A	More Details
CVE-2026-5493	Labcenter Electronics Proteus PDSPRJ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Labcenter Electronics Proteus. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDSPRJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25718.	N/A	More Details
CVE-2026-5059	aws-mcp-server AWS CLI Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of aws-mcp-server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the allowed commands list. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the MCP server. Was ZDI-CAN-27969.	N/A	More Details
CVE-2026-5058	aws-mcp-server Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of aws-mcp-server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the allowed commands list. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the MCP server. Was ZDI-CAN-27968.	N/A	More Details
CVE-2026-5055	NoMachine Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of NoMachine. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the NoMachine Device Server. The product loads a library from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-28494.	N/A	More Details
CVE-2026-5054	NoMachine External Control of File Path Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of NoMachine. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of command line parameters. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-28630.	N/A	More Details
CVE-2026-5053	NoMachine External Control of File Path Arbitrary File Deletion Vulnerability. This vulnerability allows local attackers to delete arbitrary files on affected installations of NoMachine. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of environment variables. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete files in the context of root. Was ZDI-CAN-	N/A	More Details

	28644.		
CVE-2026-4158	KeePassXC OpenSSL Configuration Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of KeePassXC. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the configuration of OpenSSL. The product loads configuration from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of KeePassXC when run by a target user on the system. Was ZDI-CAN-29156.	N/A	More Details
CVE-2026-31908	Header injection vulnerability in Apache APISIX. The attacker can take advantage of certain configuration in forward-auth plugin to inject malicious headers. This issue affects Apache APISIX: from 2.12.0 through 3.15.0. Users are recommended to upgrade to version 3.16.0, which fixes the issue.	N/A	More Details
CVE-2026-4156	ChargePoint Home Flex OCPP getpreq Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of ChargePoint Home Flex EV chargers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of OCPP messages. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-26339.	N/A	More Details
CVE-2026-4155	ChargePoint Home Flex Inclusion of Sensitive Information in Source Code Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of ChargePoint Home Flex charging stations. Authentication is not required to exploit this vulnerability. The specific flaw exists within the genpw script. The issue results from the inclusion of a secret cryptographic seed value within the script. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-26340.	N/A	More Details
CVE-2026-4154	GIMP XPM File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XPM files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28901.	N/A	More Details
CVE-2026-4153	GIMP PSP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PSP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28874.	N/A	More Details
CVE-2026-4151	GIMP ANI File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ANI files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28813.	N/A	More Details
CVE-2026-31424	In the Linux kernel, the following vulnerability has been resolved: netfilter: x_tables: restrict xt_check_match/xt_check_target extensions for NFPROTO_ARP Weiming Shi says: xt_match and xt_target structs registered with NFPROTO_UNSPEC can be loaded by any protocol family through nft_compat. When such a match/target sets .hooks to restrict which hooks it may run on, the bitmask uses NF_INET_* constants. This is only correct for families whose hook layout matches NF_INET_*: IPv4, IPv6, INET, and bridge all share the same five hooks (PRE_ROUTING ... POST_ROUTING). ARP only has three hooks (IN=0, OUT=1, FORWARD=2) with different semantics. Because NF_ARP_OUT == 1 == NF_INET_LOCAL_IN, the .hooks validation silently passes for the wrong reasons, allowing matches to run on ARP chains where the hook assumptions (e.g. state->in being set on input hooks) do not hold. This leads to NULL pointer dereferences; xt_devgroup is one concrete example: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000044: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000220-0x0000000000000227] RIP: 0010:devgroup_mt+0xff/0x350 Call Trace: <TASK> nft_match_eval (net/netfilter/nft_compat.c:407) nft_do_chain (net/netfilter/nf_tables_core.c:285) nft_do_chain_arp (net/netfilter/nft_chain_filter.c:61) nf_hook_slow (net/netfilter/core.c:623) arp_xmit (net/ipv4/arp.c:666) </TASK> Kernel panic - not syncing: Fatal exception in interrupt Fix it by restricting arptables to NFPROTO_ARP extensions only. Note that arptables-legacy only supports: - arpt_CLASSIFY - arpt_mangle - arpt_MARK that provide explicit NFPROTO_ARP match/target declarations.	N/A	More Details
CVE-2026-4150	GIMP PSD File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28807.	N/A	More Details
CVE-2026-4149	Sonos Era 300 SMB Response Out-Of-Bounds Access Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sonos Era 300. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the DataOffset field within SMB responses. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the	N/A	More Details

	kernel. Was ZDI-CAN-28345.		
CVE-2026-3691	OpenClaw Client PKCE Verifier Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose stored credentials on affected installations of OpenClaw. User interaction is required to exploit this vulnerability in that the target must initiate an OAuth authorization flow. The specific flaw exists within the implementation of OAuth authorization. The issue results from the exposure of sensitive data in the authorization URL query string. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-29381.	N/A	More Details
CVE-2026-3690	OpenClaw Canvas Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of OpenClaw. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the the authentication function for canvas endpoints. The issue results from improper implementation of authentication. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-29311.	N/A	More Details
CVE-2026-3689	OpenClaw Canvas Path Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenClaw. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of the path parameters provided to the canvas gateway endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-29312.	N/A	More Details
CVE-2026-5724	The frontend gRPC server's streaming interceptor chain did not include the authorization interceptor. When a ClaimMapper and Authorizer are configured, unary RPCs enforce authentication and authorization, but the streaming AdminService/StreamWorkflowReplicationMessages endpoint accepted requests without credentials. This endpoint is registered on the same port as WorkflowService and cannot be disabled independently. An attacker with network access to the frontend port could open the replication stream without authentication. Data exfiltration is possible, but only when a configured replication target is correctly configured and the attacker has knowledge of the cluster configuration, as the history service validates cluster IDs and peer membership before returning replication data. Temporal Cloud is not affected.	N/A	More Details
CVE-2026-40252	FastGPT is an AI Agent building platform. Prior to 4.14.10.4, Broken Access Control vulnerability (IDOR/BOLA) allows any authenticated team to access and execute applications belonging to other teams by supplying a foreign appId. While the API correctly validates the team token, it does not verify that the requested application belongs to the authenticated team. This leads to cross-tenant data exposure and unauthorized execution of private AI workflows. This vulnerability is fixed in 4.14.10.4.	N/A	More Details
CVE-2026-40191	ClearanceKit intercepts file-system access events on macOS and enforces per-process access policies. Prior to 5.0.4-beta-1f46165, ClearanceKit's Endpoint Security event handler only checked the source path of dual-path file operations against File Access Authorization (FAA) rules and App Jail policies. The destination path was ignored entirely. This allowed any local process to bypass file-access protection by using rename, link, copyfile, exchangedata, or clone operations to place or replace files inside protected directories. This vulnerability is fixed in 5.0.4-beta-1f46165.	N/A	More Details
CVE-2026-40180	Quarkus OpenAPI Generator is Quarkus' extensions for generation of Rest Clients and server stubs generation. Prior to 2.16.0 and 2.15.0-lts, the unzip() method in ApicurioCodegenWrapper.java extracts ZIP entries without validating that the resolved file path stays within the intended output directory. At line 101, the destination is constructed as new File(toOutputDir, entry.getName()) and the content is written immediately. A malicious ZIP archive containing entries with path traversal sequences (e.g., ../../malicious.java) would write files outside the target directory. This vulnerability is fixed in 2.16.0 and 2.15.0-lts.	N/A	More Details
CVE-2026-40178	ajenti.plugin.core defines all necessary core elements to allow Ajenti to run properly. Prior to 0.112, if the 2FA was activated, it was possible during a short moment after the authentication of an user to bypass its authentication. This vulnerability is fixed in 0.112.	N/A	More Details
CVE-2026-40177	ajenti.plugin.core defines all necessary core elements to allow Ajenti to run properly. Prior to 0.112, if the 2FA was activated, it was possible to bypass the password authentication This vulnerability is fixed in 0.112.	N/A	More Details
CVE-2026-39922	GeoNode versions 4.0 before 4.4.5 and 5.0 before 5.0.2 contain a server-side request forgery vulnerability in the service registration endpoint that allows authenticated attackers to trigger outbound network requests to arbitrary URLs by submitting a crafted service URL during form validation. Attackers can probe internal network targets including loopback addresses, RFC1918 private IP ranges, link-local addresses, and cloud metadata services by exploiting insufficient URL validation in the WMS service handler without private IP filtering or allowlist enforcement.	N/A	More Details
CVE-2026-39921	GeoNode versions 4.0 before 4.4.5 and 5.0 before 5.0.2 contain a server-side request forgery vulnerability that allows authenticated users with document upload permissions to trigger arbitrary outbound HTTP requests by providing a malicious URL via the doc_url parameter during document upload. Attackers can supply URLs pointing to internal network targets, loopback addresses, RFC1918 addresses, or cloud metadata services to cause the server to make requests to internal resources without SSRF mitigations such as private IP filtering or redirect validation.	N/A	More Details
CVE-2026-3446	When calling base64.b64decode() or related functions the decoding process would stop after encountering the first padded quad regardless of whether there was more information to be processed. This can lead to data being accepted which may be processed differently by other implementations. Use "validate=True" to enable stricter processing of base64 data.	N/A	More Details
	Labcenter Electronics Proteus PDSPRJ File Parsing Type Confusion Remote Code Execution Vulnerability. This		

CVE-2026-5496	vulnerability allows remote attackers to execute arbitrary code on affected installations of Labcenter Electronics Proteus. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDSPRJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25717.	N/A	More Details
CVE-2026-32146	Improper path validation vulnerability in the Gleam compiler's handling of git dependencies allows arbitrary file system modification during dependency download. Dependency names from gleam.toml and manifest.toml are incorporated into filesystem paths without sufficient validation or confinement to the intended dependency directory, allowing attacker-controlled paths (via relative traversal such as ../ or absolute paths) to target filesystem locations outside that directory. When resolving git dependencies (e.g. via gleam deps download), the computed path is used for filesystem operations including directory deletion and creation. This vulnerability occurs during the dependency resolution and download phase, which is generally expected to be limited to fetching and preparing dependencies within a confined directory. A malicious direct or transitive git dependency can exploit this issue to delete and overwrite arbitrary directories outside the intended dependency directory, including attacker-chosen absolute paths, potentially causing data loss. In some environments, this may be further leveraged to achieve code execution, for example by overwriting git hooks or shell configuration files. This issue affects Gleam from 1.9.0-rc1 until 1.15.4.	N/A	More Details
CVE-2026-1116	A Cross-site Scripting (XSS) vulnerability was identified in the `from_dict` method of the `AppLollmsMessage` class in parisneo/lollms prior to version 2.2.0. The vulnerability arises from the lack of sanitization or HTML encoding of the `content` field when deserializing user-provided data. This allows an attacker to inject malicious HTML or JavaScript payloads, which can be executed in the context of another user's browser. Exploitation of this vulnerability can lead to account takeover, session hijacking, or wormable attacks.	N/A	More Details
CVE-2026-31413	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix unsound scalar forking in maybe_fork_scalars() for BPF_OR maybe_fork_scalars() is called for both BPF_AND and BPF_OR when the source operand is a constant. When dst has signed range [-1, 0], it forks the verifier state: the pushed path gets dst = 0, the current path gets dst = -1. For BPF_AND this is correct: 0 & K == 0. For BPF_OR this is wrong: 0 | K == K, not 0. The pushed path therefore tracks dst as 0 when the runtime value is K, producing an exploitable verifier/runtime divergence that allows out-of-bounds map access. Fix this by passing env->insn_idx (instead of env->insn_idx + 1) to push_stack(), so the pushed path re-executes the ALU instruction with dst = 0 and naturally computes the correct result for any opcode.	N/A	More Details
CVE-2026-31423	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_hfsc: fix divide-by-zero in rtsc_min() m2sm() converts a u32 slope to a u64 scaled value. For large inputs (e.g. m1=4000000000), the result can reach 2^32. rtsc_min() stores the difference of two such u64 values in a u32 variable `dsm` and uses it as a divisor. When the difference is exactly 2^32 the truncation yields zero, causing a divide-by-zero oops in the concave-curve intersection path: Oops: divide error: 0000 RIP: 0010:rtsc_min (net/sched/sch_hfsc.c:601) Call Trace: init_ed (net/sched/sch_hfsc.c:629) hfsc_enqueue (net/sched/sch_hfsc.c:1569) [...] Widen `dsm` to u64 and replace do_div() with div64_u64() so the full difference is preserved.	N/A	More Details
CVE-2026-31422	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_flow: fix NULL pointer dereference on shared blocks flow_change() calls tcf_block_q() and dereferences q->handle to derive a default baseclass. Shared blocks leave block->q NULL, causing a NULL deref when a flow filter without a fully qualified baseclass is created on a shared block. Check tcf_block_shared() before accessing block->q and return -EINVAL for shared blocks. This avoids the null-deref shown below: == KASAN: null-ptr-deref in range [0x0000000000000038-0x000000000000003f] RIP: 0010:flow_change (net/sched/cls_flow.c:508) Call Trace: tc_new_tfilter (net/sched/cls_api.c:2432) rtnetlink_rcv_msg (net/core/rtnetlink.c:6980) [...] ==	N/A	More Details
CVE-2026-31421	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_fw: fix NULL pointer dereference on shared blocks The old-method path in fw_classify() calls tcf_block_q() and dereferences q->handle. Shared blocks leave block->q NULL, causing a NULL deref when an empty cls_fw filter is attached to a shared block and a packet with a nonzero major skb mark is classified. Reject the configuration in fw_change() when the old method (no TCA_OPTIONS) is used on a shared block, since fw_classify()'s old-method path needs block->q which is NULL for shared blocks. The fixed null-ptr-deref calling stack: KASAN: null-ptr-deref in range [0x0000000000000038-0x000000000000003f] RIP: 0010:fw_classify (net/sched/cls_fw.c:81) Call Trace: tcf_classify (./include/net/tc_wrapper.h:197 net/sched/cls_api.c:1764 net/sched/cls_api.c:1860) tc_run (net/core/dev.c:4401) __dev_queue_xmit (net/core/dev.c:4535 net/core/dev.c:4790)	N/A	More Details
CVE-2026-31420	In the Linux kernel, the following vulnerability has been resolved: bridge: mrp: reject zero test interval to avoid OOM panic br_mrp_start_test() and br_mrp_start_in_test() accept the user-supplied interval value from netlink without validation. When interval is 0, usecs_to_jiffies(0) yields 0, causing the delayed work (br_mrp_test_work_expired / br_mrp_in_test_work_expired) to reschedule itself with zero delay. This creates a tight loop on system_percpu_wq that allocates and transmits MRP test frames at maximum rate, exhausting all system memory and causing a kernel panic via OOM deadlock. The same zero-interval issue applies to br_mrp_start_in_test_parse() for interconnect test frames. Use NLA_POLICY_MIN(NLA_U32, 1) in the nla_policy tables for both IFLA_BRIDGE_MRP_START_TEST_INTERVAL and IFLA_BRIDGE_MRP_START_IN_TEST_INTERVAL, so zero is rejected at the netlink attribute parsing layer before the value ever reaches the workqueue scheduling code. This is consistent with how other bridge subsystems (br_fdb, br_mst) enforce range constraints on netlink attributes.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net: bonding: fix use-after-free in bond_xmit_broadcast() bond_xmit_broadcast() reuses the original skb for the last slave (determined by		

CVE-2026-31419	bond_is_last_slave()) and clones it for others. Concurrent slave enslave/release can mutate the slave list during RCU-protected iteration, changing which slave is "last" mid-loop. This causes the original skb to be double-consumed (double-freed). Replace the racy bond_is_last_slave() check with a simple index comparison (i + 1 == slaves_count) against the pre-snapshot slave count taken via READ_ONCE() before the loop. This preserves the zero-copy optimization for the last slave while making the "last" determination stable against concurrent list mutations. The UAF can trigger the following crash: == BUG: KASAN: slab-use-after-free in skb_clone Read of size 8 at addr ffff888100ef8d40 by task exploit/147 CPU: 1 UID: 0 PID: 147 Comm: exploit Not tainted 7.0.0-rc3+ #4 PREEMPTLAZY Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123) print_report (mm/kasan/report.c:379 mm/kasan/report.c:482) kasan_report (mm/kasan/report.c:597) skb_clone (include/linux/skbuff.h:1724 include/linux/skbuff.h:1792 include/linux/skbuff.h:3396 net/core/skbuff.c:2108) bond_xmit_broadcast (drivers/net/bonding/bond_main.c:5334) bond_start_xmit (drivers/net/bonding/bond_main.c:5567 drivers/net/bonding/bond_main.c:5593) dev_hard_start_xmit (include/linux/netdevice.h:5325 include/linux/netdevice.h:5334 net/core/dev.c:3871 net/core/dev.c:3887) __dev_queue_xmit (include/linux/netdevice.h:3601 net/core/dev.c:4838) ip6_finish_output2 (include/net/neighbour.h:540 include/net/neighbour.h:554 net/ipv6/ip6_output.c:136) ip6_finish_output (net/ipv6/ip6_output.c:208 net/ipv6/ip6_output.c:219) ip6_output (net/ipv6/ip6_output.c:250) ip6_send_skb (net/ipv6/ip6_output.c:1985) udp_v6_send_skb (net/ipv6/udp.c:1442) udpv6_sendmsg (net/ipv6/udp.c:1733) __sys_sendto (net/socket.c:730 net/socket.c:742 net/socket.c:2206) __x64_sys_sendto (net/socket.c:2209) 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:130) </TASK> Allocated by task 147: Freed by task 147: The buggy address belongs to the object at ffff888100ef8c80 which belongs to the cache skbuff_head_cache of size 224 The buggy address is located 192 bytes inside of freed 224-byte region [ffff888100ef8c80, ffff888100ef8d60) Memory state around the buggy address: ffff888100ef8c00: fb fb fb fb fc fc fc fc fc fc fc fc fc fc fc fc ffff888100ef8c80: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff888100ef8d00: fb fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ^ ffff888100ef8d80: fc fc fc fc fc fc fc fc fa fb fb fb fb fb fb fb ffff888100ef8e00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ==	N/A	More Details
CVE-2026-31418	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: drop logically empty buckets in mtype_del mtype_del() counts empty slots below n->pos in k, but it only drops the bucket when both n->pos and k are zero. This misses buckets whose live entries have all been removed while n->pos still points past deleted slots. Treat a bucket as empty when all positions below n->pos are unused and release it directly instead of shrinking it further.	N/A	More Details
CVE-2026-31417	In the Linux kernel, the following vulnerability has been resolved: net/x25: Fix overflow when accumulating packets Add a check to ensure that `x25_sock.fraglen` does not overflow. The `fraglen` also needs to be resetted when purging `fragment_queue` in `x25_clear_queues()`.	N/A	More Details
CVE-2026-31416	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_log: account for netlink header size This is a followup to an old bug fix: NLMSG_DONE needs to account for the netlink header size, not just the attribute size. This can result in a WARN splat + drop of the netlink message, but other than this there are no ill effects.	N/A	More Details
CVE-2026-31415	In the Linux kernel, the following vulnerability has been resolved: ipv6: avoid overflows in ip6_datagram_send_ctl() Yiming Qian reported : <quote> I believe I found a locally triggerable kernel bug in the IPv6 sendmsg ancillary-data path that can panic the kernel via `skb_under_panic()` (local DoS). The core issue is a mismatch between: - a 16-bit length accumulator (`struct ipv6_txoptions::opt_flen`, type `__u16`) and - a pointer to the *last* provided destination-options header (`opt->dst1opt`) when multiple `IPV6_DSTOPTS` control messages (cmsgs) are provided. - `include/net/ipv6.h`: - `struct ipv6_txoptions::opt_flen` is `__u16` (wrap possible). (lines 291-307, especially 298) - `net/ipv6/datagram.c:ip6_datagram_send_ctl()`: - Accepts repeated `IPV6_DSTOPTS` and accumulates into `opt_flen` without rejecting duplicates. (lines 909-933) - `net/ipv6/ip6_output.c:__ip6_append_data()`: - Uses `opt->opt_flen + opt->opt_nflen` to compute header sizes/headroom decisions. (lines 1448-1466, especially 1463-1465) - `net/ipv6/ip6_output.c:__ip6_make_skb()`: - Calls `ipv6_push_frag_opts()` if `opt->opt_flen` is non-zero. (lines 1930-1934) - `net/ipv6/exthdrs.c:ipv6_push_frag_opts()` / `ipv6_push_exthdr()`: - Push size comes from `ipv6_optlen(opt->dst1opt)` (based on the pointed-to header). (lines 1179-1185 and 1206-1211) 1. `opt_flen` is a 16-bit accumulator: - `include/net/ipv6.h:298` defines `__u16 opt_flen; /* after fragment hdr */`. 2. `ip6_datagram_send_ctl()` accepts *repeated* `IPV6_DSTOPTS` cmsgs and increments `opt_flen` each time: - In `net/ipv6/datagram.c:909-933`, for `IPV6_DSTOPTS`: - It computes `len = ((hdr->hdrlen + 1) << 3);` - It checks `CAP_NET_RAW` using `ns_capable(net->user_ns, CAP_NET_RAW)`. (line 922) - Then it does: - `opt->opt_flen += len;` (line 927) - `opt->dst1opt = hdr;` (line 928) There is no duplicate rejection here (unlike the legacy `IPV6_2292DSTOPTS` path which rejects duplicates at `net/ipv6/datagram.c:901-904`). If enough large `IPV6_DSTOPTS` cmsgs are provided, `opt_flen` wraps while `dst1opt` still points to a large (2048-byte) destination-options header. In the attached PoC (`poc.c`): - 32 cmsgs with `hdrlen=255` => `len = (255+1)*8 = 2048` - 1 cmsg with `hdrlen=0` => `len = 8` - Total increment: `32*2048 + 8 = 65544`, so `(__u16)opt_flen == 8` - The last cmsg is 2048 bytes, so `dst1opt` points to a 2048-byte header. 3. The transmit path sizes headers using the wrapped `opt_flen`: - In `net/ipv6/ip6_output.c:1463-1465`: - `headersize = sizeof(struct ipv6hdr) + (opt ? opt->opt_flen + opt->opt_nflen : 0) + ...;` With wrapped `opt_flen`, `headersize`/headroom decisions underestimate what will be pushed later. 4. When building the final skb, the actual push length comes from `dst1opt` and is not limited by wrapped `opt_flen`: - In `net/ipv6/ip6_output.c:1930-1934`: - `if (opt->opt_flen) proto = ipv6_push_frag_opts(skb, opt, proto);` - In `net/ipv6/exthdrs.c:1206-1211`, `ipv6_push_frag_opts()` pushes `dst1opt` via `ipv6_push_exthdr()`. - In `net/ipv6/exthdrs.c:1179-1184`, `ipv6_push_exthdr()` does: - `skb_push(skb, ipv6_optlen(opt));` - `memcpy(h, opt, ipv6_optlen(opt));` With insufficient headroom, `skb_push()` underflows and triggers `skb_under_panic()` -> `BUG()`: - `net/core/skbuff.c:2669-2675` (`skb_push()` calls `skb_under_panic()`) - `net/core/skbuff.c:207-214` (`skb_panic()` ends in `BUG()`) - The `IPV6_DSTOPTS` cmsg path requires `CAP_NET_RAW` in the target netns user namespace (`ns_capable(net->user_ns, CAP_NET_RAW)`). - Root (or any task with `CAP_NET_RAW`) can trigger this without user	N/A	More Details

	namespaces. - An unprivileged `uid=1000` user can trigger this if unprivileged user namespaces are enabled and it can create a userns+netns to obtain namespaced `CAP_NET_RAW` (the attached PoC does this). - Local denial of service: kernel BUG/panic (system crash). - ---truncated---		
CVE-2026-31414	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_expect: use expect->helper Use expect->helper in ctnetlink and /proc to dump the helper name. Using nfct_help() without holding a reference to the master conntrack is unsafe. Use exp->master->helper in ctnetlink path if userspace does not provide an explicit helper when creating an expectation to retain the existing behaviour. The ctnetlink expectation path holds the reference on the master conntrack and nf_conntrack_expect lock and the nfnetlink glue path refers to the master ct that is attached to the skb.	N/A	More Details
CVE-2026-6204	LibreNMS versions before 26.3.0 are affected by an authenticated remote code execution vulnerability by abusing the Binary Locations config and the Netcommand feature. Successful exploitation requires administrative privileges. Exploitation could result in compromise of the underlying web server.	N/A	More Details
CVE-2026-2728	LibreNMS versions before 26.3.0 are affected by an authenticated Cross-site Scripting vulnerability on the showconfig page. Successful exploitation requires administrative privileges. Exploitation could result in XSS attacks being performed against other users with access to the page.	N/A	More Details
CVE-2026-4810	A Code Injection and Missing Authentication vulnerability in Google Agent Development Kit (ADK) versions 1.7.0 (and 2.0.0a1) through 1.28.1 (and 2.0.0a2) on Python (OSS), Cloud Run, and GKE allows an unauthenticated remote attacker to execute arbitrary code on the server hosting the ADK instance. This vulnerability was patched in versions 1.28.1 and 2.0.0a2. Customers need to redeploy the upgraded ADK to their production environments. In addition, if they are running ADK Web locally, they also need to upgrade their local instance.	N/A	More Details
CVE-2026-0234	An improper verification of cryptographic signature vulnerability exists in Cortex XSOAR and Cortex XSIAM platforms during integration of Microsoft Teams that enables an unauthenticated user to access and modify protected resources.	N/A	More Details
CVE-2026-0233	A certificate validation vulnerability in Palo Alto Networks Autonomous Digital Experience Manager on Windows allows an unauthenticated attacker with adjacent network access to execute arbitrary code with NT AUTHORITY\SYSTEM privileges.	N/A	More Details
CVE-2026-0232	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows allows a local Windows administrator to disable the agent. This issue may be leveraged by malware to perform malicious activity without detection.	N/A	More Details
CVE-2026-34865	Out-of-bounds write vulnerability in the WEB module.Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	N/A	More Details
CVE-2026-21014	Improper access control in Samsung Camera prior to version 16.5.00.28 allows local attacker to access location data. User interaction is required for triggering this vulnerability.	N/A	More Details
CVE-2026-21013	Incorrect default permission in Galaxy Wearable prior to version 2.2.68.26 allows local attackers to access sensitive information.	N/A	More Details
CVE-2026-21009	Improper check for exceptional conditions in Recents prior to SMR Apr-2026 Release 1 allows physical attacker to bypass App Pinning.	N/A	More Details
CVE-2026-21003	Improper input validation in data related to network restrictions prior to SMR Apr-2026 Release 1 allows physical attackers to bypass the restrictions.	N/A	More Details
CVE-2026-6179	Stored Cross Site Scripting in NightWolf Penetration Testing Platform allows attack trigger and run malicious script in user's browser	N/A	More Details
CVE-2026-4402	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-5600	A new API endpoint introduced in pretix 2025 that is supposed to return all check-in events of a specific event in fact returns all check-in events belonging to the respective organizer. This allows an API consumer to access information for all other events under the same organizer, even those they should not have access to. These records contain information on the time and result of every ticket scan as well as the ID of the matched ticket. Example: { "id": 123, "successful": true, "error_reason": null, "error_explanation": null, "position": 321, "datetime": "2020-08-23T09:00:00+02:00", "list": 456, "created": "2020-08-23T09:00:00+02:00", "auto_checked_in": false, "gate": null, "device": 1, "device_id": 1, "type": "entry" } An unauthorized user usually has no way to match these IDs (position) back to individual people.	N/A	More Details
	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric GENESIS64 versions 10.97.3 and prior, Mitsubishi Electric ICONICS Suite versions 10.97.3 and prior, Mitsubishi Electric MobileHMI versions 10.97.3 and prior, Mitsubishi Electric Hyper Historian versions 10.97.3 and prior, Mitsubishi Electric AnalytiX versions 10.97.3 and prior,		

CVE-2025-14815	Mitsubishi Electric GENESIS versions 11.02 and prior, Mitsubishi Electric MC Works64 all versions, Mitsubishi Electric Iconics Digital Solutions GENESIS64 versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions ICONICS Suite versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions MobileHMI versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions Hyper Historian versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions AnalytiX versions 10.97.3 and prior, and Mitsubishi Electric Iconics Digital Solutions GENESIS versions 11.02 and prior allows a local attacker to disclose the SQL Server credentials stored in plaintext within the local SQLite file by exploiting this vulnerability, when the local caching feature using SQLite is enabled and SQL authentication is used for the SQL Server authentication. As a result, the unauthorized attacker could access the SQL Server and disclose, tamper with, or destroy data on the server, potentially cause a denial-of-service (DoS) condition on the system.	N/A	More Details
CVE-2025-14816	Cleartext Storage of Sensitive Information in GUI vulnerability in Mitsubishi Electric GENESIS64 versions 10.97.3 and prior, Mitsubishi Electric ICONICS Suite versions 10.97.3 and prior, Mitsubishi Electric MobileHMI versions 10.97.3 and prior, Mitsubishi Electric Hyper Historian versions 10.97.3 and prior, Mitsubishi Electric AnalytiX versions 10.97.3 and prior, Mitsubishi Electric GENESIS versions 11.02 and prior, Mitsubishi Electric MC Works64 all versions, Mitsubishi Electric Iconics Digital Solutions GENESIS64 versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions ICONICS Suite versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions MobileHMI versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions Hyper Historian versions 10.97.3 and prior, Mitsubishi Electric Iconics Digital Solutions AnalytiX versions 10.97.3 and prior, and Mitsubishi Electric Iconics Digital Solutions GENESIS versions 11.02 and prior allows a local attacker to disclose the SQL Server credentials displayed in plain text in the GUI of the Hyper Historian Splitter feature by exploiting this vulnerability, when SQL authentication is used for the SQL Server authentication. As a result, the unauthorized attacker could access the SQL Server and disclose, tamper with, or destroy data on the server, potentially cause a denial-of-service (DoS) condition on the system.	N/A	More Details
CVE-2026-39602	Missing Authorization vulnerability in Rustaurius Order Tracking order-tracking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Order Tracking: from n/a through <= 3.4.3.	N/A	More Details
CVE-2026-31411	In the Linux kernel, the following vulnerability has been resolved: net: atm: fix crash due to unvalidated vcc pointer in sigd_send() Reproducer available at [1]. The ATM send path (sendmsg -> vcc_sendmsg -> sigd_send) reads the vcc pointer from msg->vcc and uses it directly without any validation. This pointer comes from userspace via sendmsg() and can be arbitrarily forged: int fd = socket(AF_ATMSVC, SOCK_DGRAM, 0); ioctl(fd, ATMSIGD_CTRL); // become ATM signaling daemon struct msghdr msg = { .msg_iov = &iov, ... }; *(unsigned long *)(buf + 4) = 0xdeadbeef; // fake vcc pointer sendmsg(fd, &msg, 0); // kernel dereferences 0xdeadbeef In normal operation, the kernel sends the vcc pointer to the signaling daemon via sigd_enq() when processing operations like connect(), bind(), or listen(). The daemon is expected to return the same pointer when responding. However, a malicious daemon can send arbitrary pointer values. Fix this by introducing find_get_vcc() which validates the pointer by searching through vcc_hash (similar to how sigd_close() iterates over all VCCs), and acquires a reference via sock_hold() if found. Since struct atm_vcc embeds struct sock as its first member, they share the same lifetime. Therefore using sock_hold/sock_put is sufficient to keep the vcc alive while it is being used. Note that there may be a race with sigd_close() which could mark the vcc with various flags (e.g., ATM_VF_RELEASED) after find_get_vcc() returns. However, sock_hold() guarantees the memory remains valid, so this race only affects the logical state, not memory safety. [1]: https://gist.github.com/mrpre/1ba5949c45529c511152e2f4c755b0f3	N/A	More Details
CVE-2026-39409	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.12, ipRestriction() does not canonicalize IPv4-mapped IPv6 client addresses (e.g. ::ffff:127.0.0.1) before applying IPv4 allow or deny rules. In environments such as Node.js dual-stack, this can cause IPv4 rules to fail to match, leading to unintended authorization behavior. This vulnerability is fixed in 4.12.12.	N/A	More Details
CVE-2026-33092	Local privilege escalation due to improper handling of environment variables. The following products are affected: Acronis True Image OEM (macOS) before build 42571, Acronis True Image (macOS) before build 42902.	N/A	More Details