

Security Bulletin 07 October 2026

Generated on 07 October 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-2026-104610	A security vulnerability has been detected in Tenda HG7, HG9 and HG10 300001138_en_xpon. This impacts the function boaGetVar of the file /boaform/formLoopBack of the component Boa Web Server. Such manipulation of the argument Ethtype leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	10.0	More Details
CVE-2026-103956	Missing authentication for critical function in the authentication dependency in Loom for AWS before 1.6.1 allowed remote actors to obtain super-admin authority over the agent control plane, including registering tool servers, reading stored integration credentials, and rewriting the IAM role policies attached to managed agent roles, via any request to the application API in a deployment where no identity provider is configured. To remediate this issue, users should upgrade to version 1.6.1 or later.	10.0	More Details
CVE-2026-101148	The BackupSheep WordPress Backup Plugin WordPress plugin through 1.8 does not properly validate its integration key, treating an unset or blank key as valid, which allows unauthenticated attackers to create and download full site backups, including the database with user password hashes, and to delete arbitrary files on the server, leading to sensitive data disclosure and site takeover. The BackupSheep WordPress Backup Plugin WordPress plugin through 1.8 has been closed on WordPress.org since July 2024 and no fixed version is available. Remove it from any site where it is installed.	10.0	More Details
CVE-2026-105134	A flaw has been found in Ahsay AhsayCBS up to 10.3.2. This vulnerability affects unknown code of the file /rps/api/json/UpdateReceivers.do of the component Replication Receiver. Executing a manipulation of the argument random can lead to os command injection. It is possible to launch the attack remotely. The exploit has been published and may be used. Upgrading to version 10.3.4 is able to resolve this issue. Upgrading the affected component is advised.	10.0	More Details
CVE-2026-105135	A vulnerability has been found in InternLM MindSearch 0.1.0. This issue affects the function ExecutionAction.run of the file mindsearch/agent/graph.py of the component Planner Agent. The manipulation of the argument inputs leads to code injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
	A weakness has been identified in Totolink A3002MU 1.0.0-B20230403.1455. The impacted element		

CVE-2026-105284	is the function sub_40FCFC of the file /bin/boa of the component Authentication Check. Executing a manipulation can lead to improper authorization. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	10.0	More Details
CVE-2026-105285	A security vulnerability has been detected in Totolink A3002MU 1.0.0-B20230403.1455. This affects an unknown function of the file /boafrm/formlpQoS of the component QoS Rule Handler. The manipulation of the argument addQoS/comment/entry_name leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	10.0	More Details
CVE-2026-55107	Kobako is a Ruby gem that embeds a Wasm-isolated mruby interpreter inside applications, allowing execution of untrusted Ruby scripts (LLM-generated code, user formulas, student submissions, third-party plugins) in-process without giving them access to host memory, files, network, or credentials. From version 0.1.0 to before version 0.9.1, a guest mruby script running inside the Kobako sandbox can execute arbitrary Ruby in the host process, fully escaping the sandbox. This issue has been patched in version 0.9.1.	10.0	More Details
CVE-2026-102427	Joomla Extension - ordasoft.com - Unauthenticated Remote Code Execution in OrdaSoft Joomla CCK < 8.3.16 - site/uploader.php is reached through the component's normal frontend routing (task=getContent), a task with no authentication or ACL check anywhere in the dispatch chain. The handler validates the uploaded file's content with a real magic-byte MIME check, but the extension allow-list that would otherwise restrict the saved file's extension was present in the source and commented out. The saved file's extension was taken directly from the attacker-supplied filename with no validation, and the file was written to a path directly under the Joomla web root that is executed by the PHP handler. An image/PHP polyglot, a file whose header bytes satisfy the MIME check with PHP source appended after, passed the content check while carrying a .php extension of the attacker's choosing.	10.0	More Details
CVE-2026-96349	Unauthenticated Remote Code Execution (RCE) in SiteSkite <= 2.1.8 versions.	10.0	More Details
CVE-2026-105636	Plane is an open-source project management tool. Prior to 1.4.0, the webhook delivery task in apps/api/plane/bgtasks/webhook_task.py calls requests.post() without allow_redirects=False and does not validate redirect targets. validate_url() blocks private, loopback, link-local, and reserved addresses in the original webhook URL, but the final URL reached after one or more redirects is not checked. A user who can create a workspace can register a webhook pointing to an attacker-controlled public endpoint that returns a 302 redirect to an internal address. The Plane worker then fetches internal resources, including cloud metadata, and stores the response body in webhook_logs, where the attacker can retrieve it through the workspace webhook-logs API. This issue is fixed in 1.4.0.	9.9	More Details
CVE-2026-90970	GitLab has remediated a vulnerability in the GitLab AI Gateway component affecting all versions of the AI Gateway from 18.1.6 before 19.2.4, 19.3 before 19.3.2, and 19.4 before 19.4.1 that, under certain conditions, could have allowed an authenticated user with Duo Agent Platform access to escape the prompt template sandbox via a specially crafted flow configuration, resulting in arbitrary command execution on the AI Gateway.	9.9	More Details
CVE-2026-96658	A flaw was found in Foreman. An authenticated attacker with low-level permissions can achieve remote code execution (RCE) by bypassing the safemode sandbox within the templating engine. Due to improper handling of delegated methods, an attacker can append unauthorized functions to the allowed execution list, enabling them to run arbitrary commands on the hosting server.	9.9	More Details
CVE-2026-79901	In deployments using BoKS keytab management, affected versions of boks_keytabmd generate Active Directory service-account passwords from a predictable pseudo-random sequence seeded with the current Unix timestamp. An attacker who knows the service principal and can estimate the password-change time can reproduce a limited candidate set and verify candidates offline.	9.9	More Details
CVE-2026-82041	UTMStack before 11.2.16 contains a missing authorization vulnerability in UTMIncidentCommandWebsocket.processCommand(), the handler mapped to the /command/{hostname} STOMP destination, where no role check or command allowlist is applied before forwarding supplied commands. Any authenticated user, regardless of role, can send arbitrary operating-system commands over gRPC to any connected agent, resulting in command execution on monitored endpoints where agent processes commonly run as root or SYSTEM.	9.9	More Details
CVE-2026-105080	In ConvertX before 0.19.0, converters/calibre.ts does not block recipe files, and instead passes them to the ebook-convert program from Calibre. This affects executable code in a .recipe or .downloaded_recipe file.	9.9	More Details
	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.0, any		

CVE-2026-105740	authenticated Langflow user can achieve Remote Code Execution (RCE) on the server by adding an MCP server with the "Stdio" transport. The user-supplied command field is passed directly to bash -c "exec {command}" with zero validation, no allowlisting, and no sandboxing. The command executes immediately when the server list is fetched. Additionally, the env field allows arbitrary environment variable injection (e.g., LD_PRELOAD, PATH override). This vulnerability is fixed in 1.9.0.	9.9	More Details
CVE-2026-105697	Langflow is a tool for building and deploying AI-powered agents and workflows. Before Langflow 1.10.3, the MCP stdio transport launched whatever command / args a user put in an MCP server configuration, with no allowlist and (before 1.10.3) wrapped in bash -c "exec {command} ...". Any user able to reach the MCP server settings ("Settings → MCP Servers → Add MCP Server", POST/PATCH /api/v2/mcp/servers/{server_name}) or to build a flow with the MCP Tools component could add a "server" whose command is an arbitrary OS command (touch, rm -rf, a reverse shell, ...). The command runs on the Langflow host as the Langflow process user as soon as Langflow tries to connect to the server (listing servers, loading tools, running the flow) — even when the UI then reports that the stdio server failed to start. With the default LANGFLOW_AUTO_LOGIN=true, GET /api/v1/auto_login hands out a token without credentials, so on an exposed instance running the default configuration this is reachable without an account. AUTO_LOGIN is documented as a development-only setting; with it disabled, any authenticated (non-admin) user can exploit it. This issue is fixed in Langflow 1.10.3, langflow-base 0.10.3, and lfx 1.10.3.	9.9	More Details
CVE-2026-105691	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the SVG exporter places an attacker-controlled text object's fill-color value into a ppmcolormask command string and executes that string through child_process.exec. A user who can edit a file can store shell metacharacters in the fill color and trigger SVG export, causing commands to execute with the exporter service's privileges. The same export can be triggered through a valid public share link to a malicious file. This vulnerability is fixed in 2.18.0.	9.9	More Details
CVE-2026-102911	A flaw has been found in zosmaai pi-llm-wiki up to 0.11.7. Affected is an unknown function of the file mcp/index.ts of the component wiki_capture_source MCP tool. Executing a manipulation of the argument url can lead to os command injection. The attack can be executed remotely. The exploit has been published and may be used. Upgrading to version 0.11.8 is able to address this issue. This patch is called 360867034e79175b45c8e04a98e4ca712bbaca35. Upgrading the affected component is advised.	9.9	More Details
CVE-2026-84411	The web management service in affected RouterOS versions contains an integer underflow in its HTTP request body handling that is reachable before authentication. This can be leveraged by an unauthenticated network attacker to achieve arbitrary code execution as root, or to cause a denial of service, using a single crafted request.	9.8	More Details
CVE-2026-103110	Pexip Infinity before 38.2, plus 39.0, 39.1 and 40.0, is affected by improper input validation that allows a remote attacker to execute code remotely as an unprivileged user on a Pexip Infinity Conferencing Node.	9.8	More Details
CVE-2026-59797	Improper Privilege Management vulnerability in Apache HTTP Server's mod_ssl via SSLRequire and file-related expressions. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	9.8	More Details
CVE-2026-57941	Use After Free vulnerability in Apache HTTP Server's mod_http2 via shared session->bbtmp re-entrancy This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	9.8	More Details
CVE-2026-56154	Use After Free vulnerability in Apache HTTP Server's mod_rewrite when using lookahead (%{LA-U:HTTP:...}) This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	9.8	More Details
CVE-2026-12627	Fortra's Core Privileged Access Manager (BoKS) contains a stack-based buffer overflow vulnerability in boks_autoregisterd. A remote attacker with network access to the autoregistration service may be able to trigger memory corruption during client response processing.	9.8	More Details
CVE-2023-54405	H3C CVM, the Cloud Virtualization Management component of the H3C CAS cloud platform, contains an unauthenticated arbitrary file upload vulnerability in the /cas/fileUpload/upload endpoint that allows remote attackers to write arbitrary files by manipulating the caller-supplied token parameter without restricting path traversal or file type. Attackers can exploit the path traversal in the token parameter to upload a malicious JSP file into a web-accessible directory and then request it to achieve remote code execution as the web-server user. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-14.	9.8	More Details
CVE-2026-103752	Unauthenticated Privilege Escalation in Authorizer <= 3.15.3 versions.	9.8	More Details
	The Zella Theme WordPress theme before 2.6.3 does not perform any capability or nonce check on		

CVE-2026-75873	one of its font upload actions, which is available to unauthenticated users, allowing them to upload arbitrary files, including PHP ones, and achieve remote code execution.	9.8	More Details
CVE-2026-82825	Hitachi Coding Software Suite contains a vulnerability related to Missing Authentication for Critical Function. This allows an unauthenticated attacker to invoke a critical API, potentially leading to unauthorized retrieval or alteration of sensitive information, or unauthorized manipulation. This issue affects Hitachi Coding Software Suite: through 3.3.0.	9.8	More Details
CVE-2026-82042	UTMStack before 11.2.16 contains an authentication bypass vulnerability that allows remote attackers to gain full administrative API access by presenting a valid Utm-Internal-Key header matching the INTERNAL_KEY environment variable value, which the InternalApiKeyFilter accepts for any endpoint without path restriction, constant-time comparison, rate limiting, or audit logging. Attackers who obtain the key value can authenticate without a user account or JWT to create accounts, manage users, exfiltrate data, and modify security rules.	9.8	More Details
CVE-2026-103244	ground-station versions before 0.8.0 contain an authentication bypass vulnerability in the setup.restore command that allows unauthenticated attackers to execute arbitrary SQL during first-run setup mode. Attackers can invoke setup.restore via Socket.IO to plant admin users and forged session tokens, then authenticate as administrator without credentials for complete application takeover.	9.8	More Details
CVE-2026-75957	The Ultimate Multisite - WordPress Multisite SaaS & WaaS Platform plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.15.0 via the `checkout_form` parameter of the `login_customer_after_checkout` function. This is due to the publicly accessible `wu_ajax_nopriv_wu_validate_form` AJAX handler accepting a freely obtainable checkout nonce, and the `checkout_form=wu-finish-checkout` parameter causing `get_validation_rules()` to discard all validation rules while `finish_checkout_form_fields()` returns an empty step list — forcing `is_last_step()` to return true and routing the request directly into full order processing — after which `maybe_create_customer()` resolves the attacker-supplied `email_address` to an existing WordPress user ID without any authentication or ownership verification, and `login_customer_after_checkout()` calls `wp_set_auth_cookie()` for that user ID via a passwordless code path. This makes it possible for unauthenticated attackers to log in as any existing WordPress user — including a Network Super Admin — simply by knowing their email address. Exploitation requires that the targeted user account has no pre-existing Ultimate Multisite customer record; accounts such as a Network Super Admin on a fresh Multisite install, or any administrator or editor added before Ultimate Multisite was configured, satisfy this condition and are therefore exploitable.	9.8	More Details
CVE-2026-15989	The Super Forms - Drag & Drop Form Builder plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.3.316. This is due to the Register & Login add-on's before_email_success_msg() function whitelisting the client-submitted 'role' key and copying it into the user-data array that is passed directly to wp_insert_user(), without validating the submitted role against the administrator-configured register_user_role, without an allow-list, and without any current_user_can() capability check. This makes it possible for unauthenticated attackers to register a new account with the Administrator role by injecting role=administrator into the data submitted to any published Super Forms registration form (register_login_action='register').	9.8	More Details
CVE-2025-41753	The object name of a dynamically created BACnet File Object is interpreted as a file path without sufficient validation. Because relative paths are not limited to the intended directory, an unauthenticated remote attacker can traverse outside of it and read or overwrite arbitrary files on the device, which may lead to full system compromise.	9.8	More Details
CVE-2026-76504	A vulnerability in the API session-based authentication management of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to access an affected system with privileges of the admin user. This vulnerability is due to improper handling of URI encoding in an HTTP request, which allows the request to bypass an authentication rule that is intended to restrict access to a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted HTTP request to the API of the affected system. A successful exploit could allow the attacker to bypass authentication and gain access to the API as the admin user.	9.8	More Details
CVE-2026-82829	Hitachi Coding Software Suite contains a vulnerability related to Hidden Functionality vulnerability which allows an attacker to gain unauthorized access by exploiting hidden accounts or hard coded credentials. This issue affects Hitachi Coding Software Suite: through 3.3.0.	9.8	More Details
CVE-2026-51922	agentscope v1.0.20 contains code injection in execute_shell_command (src/agentscope/tool/_coding/_shell.py). Depending on the exposed entry, an attacker can trigger attacker-controlled code or command execution.	9.8	More Details

CVE-2026-104056	Authlib version 1.7.2 and below contains a vulnerability where discovery JSON metadata is cached without validation or issuer-origin binding. This allows a poisoned discovery response to replace all endpoint values with attacker-controlled values rather than endpoint URLs that share the origin of the configured server metadata URL.	9.8	More Details
CVE-2026-51918	FinRobot 1.0.0 contains code injection in CodingUtils.create_file_with_code ().	9.8	More Details
CVE-2026-51915	TransformerOptimus SuperAGI v0.0.14 is vulnerable to Incorrect Access Control in the tool controller. In affected source snapshots, get_tool and update_tool in superagi/controllers/tool.py accept a caller-supplied tool_id and fail to verify organization ownership through the associated toolkit. A remote authenticated attacker from one organization can read or modify another organization's tool metadata through /tools/get/{tool_id} and /tools/update/{tool_id}.	9.8	More Details
CVE-2026-94541	The WPMobile.App – Android and iOS App Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 11.82 This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to exfiltrate password-reset URLs for arbitrary users, including administrators, mirrored into the push queue by the mail-to-push feature, and use those URLs to take over the targeted accounts. This exploit chain requires the plugin's mail-to-push feature (wpmobile_auto_mail=1) to be enabled, as that setting is what causes outbound WordPress password-reset emails — including the reset URL and key — to be mirrored into the push row queue where they become accessible to the attacker.	9.8	More Details
CVE-2026-97637	The JSON API Auth plugin for WordPress is vulnerable to Authentication Bypass via Cached Session Cookie Disclosure in all versions up to, and including, 3.1.2. The vulnerability exists because the required PI-Media/json-api parent plugin caches controller dispatch results in transients keyed solely by URI and query string, ignoring HTTP method and POST body; this causes the `generate_auth_cookie()` endpoint — which embeds a live WordPress `logged_in` cookie produced by `wp_generate_auth_cookie()` directly in its JSON response body — to serve that cached authenticated response to any subsequent unauthenticated GET request to the same URI. This makes it possible for unauthenticated attackers to retrieve a valid Administrator `logged_in` session cookie from the cached response and use it to fully authenticate as the site Administrator, including via the same plugin's `get_currentuserinfo` endpoint and any cookie-authenticated controller action. Exploitation requires the PI-Media/json-api parent plugin to be installed and active with the Auth controller enabled, and a legitimate Administrator must have POSTed to `/api/auth/generate_auth_cookie/` within the preceding 24-hour cache TTL; the nominal HTTPS enforcement gate present in `Auth.php` is trivially bypassed by supplying `insecure=cool` as a request parameter.	9.8	More Details
CVE-2026-86131	A code injection vulnerability in WatchGuard Firewall OS's BOVPN Over TLS client configuration handling allows an attacker who controls the remote VPN server to execute arbitrary commands as root on the connecting Firebox.	9.8	More Details
CVE-2026-19660	The Divi Membership plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 2.3.0. The `process_paypal_callback` function, hooked to the `init` action, accepts a base64-encoded `paypal_param` GET parameter with no IPN validation, no cryptographic signature check, no ownership verification, and no nonce, allowing it to trust an entirely attacker-controlled user ID value that is passed directly to `wp_set_current_user()` and `wp_set_auth_cookie()`. This makes it possible for unauthenticated attackers to log in as any existing WordPress user — including administrators — by supplying an arbitrary user ID in the `paypal_param` GET parameter, resulting in full site takeover. The vulnerability is further compounded by the fact that the PayPal gateway class is instantiated unconditionally regardless of whether PayPal is enabled or configured, ensuring the vulnerable hook is always registered on every front-end request.	9.8	More Details
CVE-2026-14378	The DevKit Pro plugin for WordPress is vulnerable to Authentication Bypass Leading to Administrator Account Takeover in all versions up to, and including, 2.3.0 This is due to the `revert_switch` handler trusting the attacker-controlled `original_user_id` cookie as the privileged identity: `verify_nonce_and_capability()` incorrectly checks the `manage_options` capability on the user identified by the cookie rather than on the actual requester via `current_user_can()`, while the switch-back form and a valid session-bound nonce are emitted publicly via `wp_footer` to any visitor — including unauthenticated users — whenever that cookie is present. This makes it possible for unauthenticated attackers to set the `original_user_id` cookie to any administrator's user ID, collect the rendered nonce, and POST it back to the `revert_switch` handler, causing `wp_set_auth_cookie()` to be called with the administrator's ID and granting the attacker a full administrator-level authenticated session and complete site takeover.	9.8	More Details
	Mooncake transfer engine before 0.3.13 contains an untrusted pointer dereference in		

CVE-2026-103764	ServerSession::readHeader that allows unauthenticated attackers to read and write arbitrary process memory via the TCP transport data port. Attackers can send a crafted SessionHeader with arbitrary addr and size values using READ or WRITE opcodes to disclose KV cache contents, prompts and secrets or corrupt memory toward code execution.	9.8	More Details
CVE-2026-51897	RAGFlow 0.24.0 contains improper access control in get_dataset (api/apps/evaluation_app). Depending on the exposed entry, an attacker can trigger attacker-controlled code or command execution	9.8	More Details
CVE-2026-51893	infiniflow ragflow 0.24.0 is vulnerable to Incorrect Access Control via trace_mindmap. An externally reachable path accepts a caller-selected object or tenant identifier and reaches a data-access operation without a visible owner, tenant, workspace, or membership binding on that object.	9.8	More Details
CVE-2026-51886	langflow-ai langflow v1.9.3 is affected by: Code Injection. The impact is: execute arbitrary code (remote). The component is: src/backend/base/langflow/api/v1/validate.py:validate-post_validate_code-a-real-authenticated-http-post-to-api-v1. The attack vector is: Attack surface: HTTP or browser-backed service path. A public-facing route accepts raw Python source and forwards it into a server-side compile/exec validation path without any visible entitlement guard. ¶¶ A weakness has been identified in langflow-ai langflow up to 1.9.3. langflow contains a code injection vulnerability in validate-post_validate_code-a-real-authenticated-http-post-to-api-v1 (src/backend/base/langflow/api/v1/validate.py:13). An authenticated attacker can execute arbitrary Python code on the server by submitting malicious code to the /api/v1/validate/code endpoint, which directly executes user-supplied code without sandboxing or security controls.	9.8	More Details
CVE-2026-51884	The /knowledge_base/upload_temp_docs temporary document upload endpoint in Langchain Chatchat 0.3.1 is vulnerable to path traversal. By crafting malicious filenames, an attacker can write files to arbitrary locations on the server, bypassing the intended restrictions on the temporary directory.	9.8	More Details
CVE-2026-51881	deeptutor 1.4.0 contains code injection in ExecTool.execute. Through the live tutorbot WebSocket interface, a remote caller can induce the tool layer to execute reviewer-chosen shell commands in the service environment.	9.8	More Details
CVE-2026-51880	deeptutor 1.4.0 contains a path traversal issue in EditFileTool.execute. Through the live tutorbot WebSocket interface, a remote caller can induce the tool layer to write or edit absolute paths outside the intended bot workspace.	9.8	More Details
CVE-2026-104846	Seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. From 0.12.0 until 1.6.2, fromJSON deserialization of a fulfilled Promise control node can pass a plugin-produced callable-bearing thenable to a native Promise resolver. ECMAScript thenable assimilation then invokes the callable unexpectedly, allowing attacker-controlled JSON to trigger code in applications using plugin-capable Seroval releases. This path bypasses the Promise resolver type-confusion remediation in version 1.5.3 for CVE-2026-59940 because the unexpected invocation occurs through native Promise settlement after the referenced value is deserialized. This issue is fixed in version 1.6.2.	9.8	More Details
CVE-2026-51898	sinaptik-ai pandas-ai 3.0.0 is vulnerable to Code Injection in CodeExecutor.execute.	9.8	More Details
CVE-2026-51904	SuperAGI up to v0.0.14 contains an improper access control vulnerability in the agent execution controller. In affected source snapshots, create_agent_execution and create_agent_run in superagi/controllers/agent_execution.py accept a caller-supplied agent_id and fail to verify that the referenced agent belongs to the authenticated user's organization. A remote authenticated attacker from one organization can create or start execution records for agents owned by another organization through /agentexecutions/add or /agentexecutions/add_run.	9.8	More Details
CVE-2026-51911	vanna v2.0.2 contains a code injection vulnerability in VannaBase.get_plotly_figure (src/vanna/legacy/base/base.py). Depending on the exposed entry, an attacker can trigger attacker-controlled code or command execution.	9.8	More Details
CVE-2026-104286	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiMail 8.0.0 through 8.0.1, FortiMail 7.6.0 through 7.6.6, FortiMail 7.4.0 through 7.4.8, FortiMail 7.2.0 through 7.2.9 may allow an unauthenticated attacker to write arbitrary files on the underlying system via crafted HTTP or HTTPS requests.	9.8	More Details
CVE-2026-82827	Hitachi Coding Software Suite contains a vulnerability related to Use of Hard-coded Cryptographic Key. The Hardcoding of JWT signing secret key allows an attacker to generate unauthorized Bearer tokens and exploit administrative functions. This issue affects Hitachi Coding Software Suite: through 3.3.0.	9.8	More Details

CVE-2026-51870	DeepTutor v1.4.0 is vulnerable to command execution in /tutorbot/agent/tools/shell.py:ExecTool.execute.	9.8	More Details
CVE-2026-82824	Hitachi Coding Software Suite contains a vulnerability related to Path Traversal vulnerability that allows an attacker to access, create, modify, or delete files. This issue affects Hitachi Coding Software Suite: through 3.3.0.	9.8	More Details
CVE-2026-88424	FineAdmin v1.0 was discovered to contain a SQL injection vulnerability via the field/order parameter at ButtonService.GetListByFilter(). This vulnerability allows attackers to access sensitive database information via crafted SQL statements.	9.8	More Details
CVE-2026-88391	Northstar (dromara/northstar, quantitative trading platform) <= 9.1.1 enables the H2 Console but its auth interceptor only covers /northstar/**, so /h2-console is exposed with no authentication and the embedded H2 DB uses default sa / empty password. Any network-reachable attacker can run arbitrary system commands via CREATE ALIAS (pre-auth RCE).	9.8	More Details
CVE-2026-102455	EasyFlow .NET developed by Digiwin has a Insecure Deserialization vulnerability. Unauthenticated remote attackers can execute arbitrary code on the server by sending maliciously crafted serialized content.	9.8	More Details
CVE-2026-37719	An issue in dormakaba evolo Service (all versions) allows a remote attacker to execute arbitrary code as SYSTEM via a .NET component.	9.8	More Details
CVE-2026-100512	Contributor PHP Object Injection in Nested Pages <= 3.3.2 versions.	9.8	More Details
CVE-2026-88393	WookTeam v1.6.6 and before is vulnerable to RCE in the project task export interface /api/project/task/export. The data parameter is base64-decoded and passed directly into the string2array() function in app/Module/Base.php, which executes eval("\\$array = \$data;") whenever the decoded string starts with array. An attacker can inject arbitrary PHP code into the eval call and achieve RCE.	9.8	More Details
CVE-2026-55494	Tugtainer is a self-hosted app for automating updates of Docker containers. Prior to version 1.30.4, Tugtainer Agent allows unauthenticated access to Docker management APIs when AGENT_SECRET is not configured. The Agent uses request signatures to protect its API routes. However, in agent/auth.py, the signature verification function returns successfully if Config.AGENT_SECRET is empty. This causes protected Agent APIs to become accessible without authentication. This issue has been patched in version 1.30.4.	9.8	More Details
CVE-2026-88395	GouGuOA v6.0.5 and before is vulnerable to SQL Injection in /home/message/rubbish via the keywords parameter.	9.8	More Details
CVE-2026-102490	All versions of Zammad including the latest alpha enable the local zammad user to escalate privileges to root.	9.8	More Details
CVE-2026-102489	Zammad versions 6.3.0 to 6.5.4 are vulnerable a session hijack vulnerability that leads to remote code execution as the zammad user. The vulnerability is also present in version 7.0.0 to version 7.1.3, but not exploitable due to environment conditions.	9.8	More Details
CVE-2026-88920	An authentication bypass in the DOM security processor in Apache WSS4J allows unauthenticated remote attackers to forge authenticated SOAP messages via a crafted unsigned SAML sender-vouches assertion containing an attacker-controlled key. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4, which fix this issue.	9.8	More Details
CVE-2026-18782	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Trex Digital Smart Manufacturing Systems Inc. Trex MES allows Command Line Execution through SQL Injection. This issue affects Trex MES: through 2026-09-29.	9.8	More Details
CVE-2026-103395	LightLLM through 1.2.0 visual_only deployments expose an unauthenticated RPyC service with allow_pickle enabled that deserializes attacker-supplied arguments in the remote_infer_images method. Attackers can reach the visual RPyC port and pass objects with __reduce__ methods to execute arbitrary code with service account privileges.	9.8	More Details
CVE-2026-82307	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Dolusoft Software Technologies SOPLOG allows SQL Injection. This issue affects SOPLOG: before Soplog 2026.9.4.1.	9.8	More Details
CVE-2026-97274	Unauthenticated Bypass Vulnerability in OAuth Single Sign On - SSO (OAuth Client) <= 7.1.2 versions.	9.8	More Details

CVE-2026-97248	Unauthenticated PHP Object Injection in Booking Activities <= 1.18.7.1 versions.	9.8	More Details
CVE-2026-104711	Improper neutralization of special elements used in an expression language statement ('Expression Language Injection') vulnerability in Apache Struts. If the application is configured to use the legacy RESTful action mapper, a crafted request can inject an OGNL expression that may lead to remote code execution. Struts 7 is affected only when the OGNL allowlist is disabled; it is enabled by default. Applications using the default action mapper, the restful2 mapper, or the Struts REST plugin are not affected. This issue affects Apache Struts: from 2.0.0 through 2.3.37, from 2.5.0 through 2.5.33, from 6.0.0 through 6.11.0, from 7.0.0 through 7.3.0. Users are recommended to upgrade to version 6.12.0 or 7.4.0, which fixes the issue.	9.8	More Details
CVE-2026-96350	Subscriber Privilege Escalation in Estatik <= 4.3.5 versions.	9.8	More Details
CVE-2026-105641	Plane is an open-source project management tool. Prior to 1.4.0, the deployments/aio/community/ and deployments/cli/community/ manifests provide fixed, publicly known SECRET_KEY and LIVE_SERVER_SECRET_KEY defaults that remain active when operators do not override them. The top-level setup.sh randomizes secrets only for the development Docker Compose path, leaving unchanged aio and cli community deployments with shared production secrets. Knowledge of SECRET_KEY enables attackers to forge Django-signed values and compromise accounts or sessions. Knowledge of LIVE_SERVER_SECRET_KEY bypasses live-service authentication on unchanged community deployments. This issue is fixed in 1.4.0.	9.8	More Details
CVE-2026-105639	Plane is an open-source project management tool. Prior to 1.4.0, Plane's signup flow creates a logged-in User row for any submitted email without an out-of-band ownership check, while User.email is unique=True. The authenticated user can call GET /api/users/me/workspaces/invitations/, which returns each WorkspaceMemberInvite whose email matches request.user.email. WorkspaceMemberInviteSerializer uses fields = "all", exposing the token that protects the invitation join endpoint. An unauthenticated attacker who knows a target's email can register an account using that address, enumerate pending invitations, and accept an invitation as the target, joining a workspace at the invited role. The term pre-auth describes the attacker's initial state: the attacker has no credential before signup, while the enumeration and join requests use the session created by that signup. This issue is fixed in 1.4.0.	9.8	More Details
CVE-2026-105105	CWE-306: Missing Authentication for Critical Function in the ait.core.server telemetry and command broker (ait-server) in NASA-AMMOS AIT-Core through 3.1.1 allows an unauthenticated remote attacker with network access to the ZeroMQ message bus to inject spacecraft command data, exfiltrate command and telemetry traffic, inject forged telemetry, or disrupt the command and telemetry bus. The ait-server ZeroMQ broker binds its XSUB and XPUB sockets to all network interfaces by default without authentication or transport security. An attacker able to reach TCP port 5559 can publish messages onto internal topics, including the __commands__ command topic. With the shipped default configuration, command messages are forwarded through command_stream and emitted on the command-uplink UDP path. An attacker able to reach TCP port 5560 can subscribe to command and telemetry traffic on the ground bus. AIT-Core 3.1.2 changes the default ZeroMQ bind addresses to loopback.	9.8	More Details
CVE-2026-105207	ZITADEL 3.0.0 through 3.4.15 and 4.0.0 before 4.17.3 creates links between user accounts and external identity providers without verifying a primary factor or the caller's permission, including on identify-only Login V2 sessions and via the User Service V2 AddIDPLink endpoint. An unauthenticated attacker knowing a victim's login name can bind their own external IdP identity to the victim's account and then sign in as the victim.	9.8	More Details
CVE-2026-51872	Devika v1.0 is vulnerable to Code Injection via the Runner.run_code function in src/agents/runner/runner.py.	9.8	More Details
CVE-2026-102115	Kiteworks Core did not correctly validate a parameter submitted to the password reset workflow. An unauthenticated attacker who knew the email address of a user with a locally stored password could potentially reset that account's password without access to the emailed reset link and then authenticate as that user, including where the account holds administrative privileges.	9.8	More Details
CVE-2026-97283	Deserialization of Untrusted Data vulnerability in Liquid Web / StellarWP Advanced Post Manager advanced-post-manager allows Object Injection.This issue affects Advanced Post Manager: from n/a through 4.5.5.	9.8	More Details
CVE-2026-51871	Devika v1.0 is vulnerable to Code Injection in the Runner.execute function in src/agents/runner/runner.py which allows an attacker to achieve arbitrary code execution by exploiting the direct execution of LLM-generated content.	9.8	More Details

CVE-2026-19652	The Divi Membership plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 2.2.0. This is due to the <code>`dmem_form_submit_handler()`</code> function determining the new user's role by iterating all WordPress roles and calling <code>`password_verify()`</code> against an attacker-controlled bcrypt hash supplied in the <code>`form_id`</code> POST parameter, with no validation or whitelist of allowed roles. This makes it possible for unauthenticated attackers to register a new account with the administrator role by submitting a locally computed bcrypt hash of <code>`administrator`</code> as <code>`form_id`</code> , and when <code>`auto_login=on`</code> is submitted, be immediately authenticated as that administrator in the same request, resulting in full site takeover. Exploitation requires a WordPress nonce, but that nonce is publicly emitted on any page rendering the Divi Membership registration form and is therefore obtainable by any unauthenticated visitor.	9.8	More Details
CVE-2026-51856	In agentscope 1.0.18, 1.0.19, and 1.0.19 when the RealtimeAgent session exposes <code>execute_python_code</code> as an available tool, a remote WebSocket user can prompt the agent to call that tool and run Python code in the service environment. In the validated path, <code>RealtimeAgent._acting</code> forwards the model-produced tool call to <code>Toolkit.call_tool_function</code> , which invokes <code>execute_python_code</code> without an additional approval or isolation boundary on that path.	9.8	More Details
CVE-2026-51867	agentgpt v.1.0.0 is vulnerable to Incorrect Access Control in <code>next/src/server/api/routers/agentRouter.ts</code> . An externally reachable path accepts a caller-selected object or tenant identifier and reaches a data-access operation without a visible owner, tenant, workspace, or membership binding on that object.	9.8	More Details
CVE-2026-51866	In DB-GPT 0.7.5 and 0.8.0, a skill uploaded through the real <code>/api/v1/skills/upload</code> route can later be executed through the real <code>/api/v1/chat/react-agent</code> flow.	9.8	More Details
CVE-2026-51857	In camel-ai camel 0.2.91a1, v0.2.91a2 and v0.2.91a3, <code>CodeExecutionToolkit</code> can run model-produced Python code through <code>SubprocessInterpreter</code> without an approval boundary.	9.8	More Details
CVE-2026-51858	In camel-ai camel 0.2.91a1, v0.2.91a2 and v0.2.91a3, <code>TerminalToolkit.shell_exec</code> allows prompt-driven shell command execution without an approval boundary.	9.8	More Details
CVE-2026-102458	EasyFlow .NET developed by Digiwin has a Missing Authentication vulnerability. Unauthenticated remote attackers can obtain other users' plaintext passwords through a specific API.	9.8	More Details
CVE-2026-51861	bisheng 2.3.0, 2.4.0, and 2.4.0-beta1 is vulnerable to Code Injection in <code>src/backend/bisheng/api/v1/validate.py</code> .	9.8	More Details
CVE-2026-103628	Out of bounds write in WebGL in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-103626	Incorrect authorization in FileSystem in Google Chrome on on Windows prior to 154.0.8037.97 allowed a remote attacker leveraging social engineering to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-105637	Plane is an open-source project management tool. Prior to 1.4.0, <code>ProjectBulkAssetEndpoint.post</code> in <code>apps/api/plane/app/views/asset/v2.py</code> retrieves assets using <code>id_in=asset_ids</code> and <code>workspace_slug=slug</code> but does not constrain the query with <code>project_id</code> from the URL. A workspace Guest can provide asset UUIDs from another project in the same workspace and reassign their <code>issue_id</code> , <code>comment_id</code> , <code>page_id</code> , <code>draft_issue_id</code> , or <code>project_id</code> to an entity the attacker controls. Plane then treats the attacker's project as the new owner and provides a presigned download URL for the hijacked file. This issue is fixed in 1.4.0.	9.6	More Details
CVE-2026-105209	ZITADEL 3.x before 3.4.15 and 4.x before 4.17.1 contains an improper authorization vulnerability: when issuing passkey or passwordless enrollment codes, it checks only the organization in the <code>x-zitadel-orgid</code> header, not the target user's organization. Attackers with user-write permission in one organization can obtain an enrollment code for a user in another organization on the same instance and register their own authenticator to take over that account.	9.6	More Details
CVE-2026-103630	Use after free in FedCM in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-56662	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. Prior to version 1.5, the UpdateCE update form contained no anti-CSRF token, and the POST handler performed no token or request-origin verification. A remote attacker can host a page that auto-submits a forged POST to the update endpoint; when an authenticated administrator visits it, the server performs an attacker-directed download-and-deploy operation in the administrator's session — with no further interaction. Because the deployed content is executed (see the related ZIP-extraction advisory), this yields remote code execution. The url field is	9.6	More Details

	additionally written into the form unescaped, providing a secondary HTML-injection sink via a malicious upgrade.json. This issue has been patched in version 1.5.		
CVE-2026-95102	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to impersonate charging stations. As a result, attackers can exploit this weakness to gain unauthorized access to sensitive data or perform unauthorized actions. Given that no authentication is required, this can lead to privilege escalation and potentially compromise the security of the entire system.	9.4	More Details
CVE-2026-103765	Mooncake through 0.3.13.post1 contains a missing authentication vulnerability in the HTTP metadata server /metadata handler that allows unauthenticated attackers to read, overwrite, and delete transfer engine metadata keys. Attackers can poison segment descriptors such as tcp_data_port or re-create rpc_meta entries to redirect KV cache transfers to attacker-controlled listeners, or exhaust server memory.	9.4	More Details
CVE-2026-55181	Tugtainer is a self-hosted app for automating updates of Docker containers. Prior to version 1.30.3, Tugtainer's OIDC authentication can still be initiated even when OIDC_ENABLED=false. The /auth/oidc/enabled endpoint correctly reports that OIDC is disabled. However, a direct request to /auth/oidc/login still starts the OIDC login flow, returns HTTP 302, sets an oidc_state cookie, and redirects the user to the configured OIDC authorization endpoint. This bypasses the intended OIDC disable switch. This issue has been patched in version 1.30.3.	9.4	More Details
CVE-2026-102149	Kiteworks Email Protection Gateway did not sufficiently restrict which account a certificate could be assigned to. This could allow an attacker to associate a certificate with another user's account, affecting the confidentiality and integrity of that account's encrypted mail and, where certificate-based login is enabled, potentially permitting unauthorized access to the account.	9.4	More Details
CVE-2026-103352	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP BASE WP BASE Booking wp-base-booking-of-appointments-services-and-events allows Blind SQL Injection.This issue affects WP BASE Booking: from n/a through 6.4.0.	9.3	More Details
CVE-2026-103355	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Blind SQL Injection.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.20.	9.3	More Details
CVE-2026-102795	Improper Access Control vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue. This CVE supersedes CVE-2026-41920, whose record listed the affected 9.x versions as 9.0.0 through 9.1.14 and the fixed version as 9.1.15. All 9.2.x releases before 9.2.15 are affected.	9.3	More Details
CVE-2026-103922	Capacitor is a cross-platform native runtime for web applications. From 6.0.0 until 6.2.2, 7.6.9, 8.3.5, 8.4.3, and 8.5.1, the Android and iOS WebView navigation guard validates a target URL's host and scheme but not its path, allowing a victim who activates an untrusted link to navigate a frame to /_capacitor_http_interceptor_. The native proxy can fetch an attacker-selected URL and return the response as a document at the application's own origin, allowing script in that response to access same-origin storage, cookies, and registered Capacitor plugin capabilities. Applications remain affected when CapacitorHttp is disabled because affected releases serve the proxy path regardless of that setting. This issue is fixed in versions 6.2.2, 7.6.9, 8.3.5, 8.4.3, and 8.5.1.	9.3	More Details
CVE-2026-102147	A stored cross-site scripting (XSS) weakness in Kiteworks Core could allow an unauthenticated attacker to store crafted content that later executes arbitrary JavaScript in the authenticated session of an administrator who views the affected page. This could have permitted the attacker to gain full administrative control, including the creation of a new administrative account.	9.3	More Details
CVE-2026-62071	Unauthenticated SQL Injection in WordPress File Upload <= 5.1.10 versions.	9.3	More Details
CVE-2026-96822	Unauthenticated SQL Injection in Books Gallery <= 4.8.3 versions.	9.3	More Details
CVE-2026-102628	The Cadmos LTI application hosted at cadmos.eummena.io had Laravel debug mode enabled (APP_DEBUG=true, APP_ENV=local) in a publicly accessible environment. An unauthenticated attacker could send a GET request and trigger an unhandled exception, causing Laravel to expose the entire server environment, including all .env configuration variables, in plaintext. Fixed on or before 2026-09-02.	9.3	More Details
CVE-2026-	yii2-starter-kit through 4.2.0 exposes the Yii debug and Gii modules to all IP addresses by setting allowedIPs to ['*'] in its default development configuration. Unauthenticated remote attackers can	9.1	More

103475	access the debug endpoint to read sensitive data including session cookies and database queries, or access the Gii endpoint to generate and write PHP files into the application directory.		Details
CVE-2026-102106	Improper authentication in a Kiteworks Email Protection Gateway administrative service. An administrative service in Kiteworks Email Protection Gateway did not consistently enforce administrator authentication, so the required password check could be bypassed. An attacker who referenced a valid administrator account could potentially create, modify, or delete internal users and managed domains and change their security-feature configuration without authenticating; deleting a managed domain also removes its user accounts and could lock administrators out of the gateway.	9.1	More Details
CVE-2026-102105	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Server-Side Request Forgery (SSRF). A server-side request forgery (SSRF) weakness in Kiteworks Email Protection Gateway could allow a remote, unauthenticated attacker to induce the gateway to issue crafted requests to internal or otherwise unintended network destinations. The requests are triggered while the gateway renders message content that references external resources. Depending on the services reachable from the gateway, this could disclose sensitive internal information or trigger unintended actions on internal systems.	9.1	More Details
CVE-2026-102104	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Server-Side Request Forgery (SSRF). A server-side request forgery (SSRF) weakness in Kiteworks Email Protection Gateway could allow a remote, unauthenticated attacker to induce the gateway to issue crafted requests to internal or otherwise unintended network destinations. The requests are triggered while the gateway performs an online certificate status check for an inbound message. Depending on the services reachable from the gateway, this could disclose sensitive internal information or disrupt gateway operation.	9.1	More Details
CVE-2026-105215	ZITADEL before 3.4.14 and 4.x before 4.16.2 contains an authentication bypass in the hosted Login V1 UI because the 'external account not found' registration endpoint trusts client-supplied external identity fields without a completed IdP callback. Unauthenticated attackers can submit forged IDPConfigID and ExternalUserID values to pre-create an account bound to a victim's external IdP identity, which the victim's later genuine external login then signs into.	9.1	More Details
CVE-2017-20285	YAML versions before 1.30 for Perl allow a loaded document to trigger the DESTROY method of arbitrary classes. A perl/hash:Class tag blesses a hash into the class it names. The document supplies the object's fields, and Perl calls DESTROY when it goes out of scope. What DESTROY does depends on the classes the process has loaded. With File::Temp::Dir from core Perl, it can delete a directory tree the document names.	9.1	More Details
CVE-2026-102103	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Server-Side Request Forgery (SSRF). A server-side request forgery (SSRF) weakness in Kiteworks Email Protection Gateway could allow a remote, unauthenticated attacker to induce the gateway to issue crafted requests to internal or otherwise unintended network destinations. The requests are triggered while the gateway retrieves a certificate revocation list in an inbound message. Depending on the services reachable from the gateway, this could disclose sensitive internal information or disrupt gateway operation.	9.1	More Details
CVE-2026-102102	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Server-Side Request Forgery (SSRF). A server-side request forgery (SSRF) weakness in Kiteworks Email Protection Gateway could allow a remote, unauthenticated attacker to induce the gateway to issue crafted requests to internal or otherwise unintended network destinations. The requests are triggered while the gateway retrieves an issuer certificate in an inbound message. Depending on the services reachable from the gateway, this could disclose sensitive internal information or disrupt gateway operation.	9.1	More Details
CVE-2026-102095	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Server-Side Request Forgery. Kiteworks Email Protection Gateway performed server-side fetches of URLs contained in the message content it processed, without adequately restricting the fetch destination. A remote, unauthenticated sender could craft a message that caused the gateway to issue requests to internal services and cloud instance metadata endpoints and return the responses, potentially disclosing sensitive internal data and, depending on the internal service reached, affecting its state.	9.1	More Details
CVE-2026-104611	A vulnerability was detected in Tenda AC9 15.03.02.13. Affected is an unknown function of the file /goform/fast_setting_internet_set of the component POST Request Handler. Performing a manipulation of the argument netWanType results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	9.1	More Details
	Tugtainer is a self-hosted app for automating updates of Docker containers. Prior to version 1.30.6, Tugtainer allows an authenticated user to make the backend server send outbound HTTP requests		

CVE-2026-62308	to arbitrary user-supplied URLs through the notification test endpoint. The /settings/test_notification endpoint accepts a urls field and passes it directly to Apprise without restricting protocols, hostnames, localhost addresses, private IP ranges, or cloud metadata addresses. This can be abused as an authenticated blind server-side request forgery (SSRF). This issue has been patched in version 1.30.6.	9.1	More Details
CVE-2026-15896	The Super Forms – Drag & Drop Form Builder plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.3.316 via the parse_request function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. The optional 'file_upload_auth' setting defaults to empty, meaning no authentication is required in the default configuration; enabling this setting mitigates unauthenticated exploitation but does not remediate the path traversal itself. Exploitation on Linux requires a real 13-digit timestamp directory to exist, whereas on Windows the traversal works with any hardcoded 13-digit prefix. However, the plugin's file upload response returns the name of the created directory, which means the vulnerability is exploitable as long as file upload is enabled on the form.	9.1	More Details
CVE-2026-89238	WSS4J EncryptedHeader child confusion could promote an attacker-controlled plaintext element as the decrypted header, leading to incorrect confidentiality coverage and possible policy bypass. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4, which fix this issue.	9.1	More Details
CVE-2026-105638	Plane is an open-source project management tool. Prior to 1.4.0, Plane's magic-code email login uses a six-digit numeric OTP with approximately 20 bits of entropy. The verifier has no per-code failed-attempt counter, and an incorrect code does not increment a counter, invalidate the Redis entry, or lock the email address. The verifier extends django.views.View rather than DRF's APIView, so the configured AnonRateThrottle limit does not apply. The middleware stack also contains no Django-level rate limiter such as django-ratelimit, django-axes, or an IP-throttling middleware. This vulnerability is fixed in 1.4.0.	9.1	More Details
CVE-2026-87830	In the StAX streaming WS-SecurityPolicy validator, certain relative or unsupported XPath expressions can be converted into paths that never match the actual XML element path. A remote SOAP peer may therefore send a required element without the expected signature or encryption. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4, which fix this issue.	9.1	More Details
CVE-2026-105640	Plane is an open-source project management tool. Prior to 1.4.0, Plane trusts email addresses returned by Gitea OAuth and by self-managed GitLab OAuth deployments where email confirmation is disabled, without verifying that the provider authenticated ownership of the address. An attacker can set an OAuth identity's unverified provider email to a victim's address, which Plane matches directly to the victim's existing local account. The attacker can then log in to the victim's Plane account without knowing the victim's password. GitHub, GitLab.com, and Google are not affected because those providers return verified email addresses. This issue is fixed in 1.4.0.	9.1	More Details
CVE-2026-94053	Authentication bypass via LDAP injection in component sshd-ldap in Apache MINA SSHD versions 1.2.0 to 2.19.0 and 3.0.0-M1 to 3.0.0-M5. Apache MINA SSHD is a Java library for client-side and server-side SSH. The optional sshd-ldap component provides support for integrating password and publickey authentication on the server side with an LDAP server. sshd-ldap is an optional component. SSH servers implemented with Apache MINA SSHD are affected only if they use sshd-ldap and do configure it to be used for password or public key authentication. Other Apache MINA SSHD servers are not affected. Lack of escaping LDAP filter metacharacters enabled successful authentication with username "*" and password "*". Users are recommended to upgrade affected applications to version 2.20.0 or 3.0.0-M6, which fix this issue by properly escaping filter parameters according to RFC 4515.	9.1	More Details
CVE-2026-94052	A missing check in LdapPasswordAuthenticator in component sshd-ldap in Apache MINA SSHD versions 1.2.0 to 2.19.0 or 3.0.0-M1 to 3.0.0-M5 bypassed authentication checks. Apache MINA SSHD is a Java library for client-side and server-side SSH. The optional sshd-ldap component provides support for integrating password and publickey authentication on the server side with an LDAP server. sshd-ldap is an optional component. SSH servers implemented with Apache MINA SSHD are affected only if they use sshd-ldap and do configure an LdapPasswordAuthenticator to be used for password authentication. Normal password authentication via the built-in mechanisms in sshd-core is _not_ affected by this vulnerability, which concerns only LdapPasswordAuthenticator. Users are recommended to upgrade affected applications to version 2.20.0 or 3.0.0-M6, which fix this issue.	9.1	More Details
	Authentication bypass in sshd-core in Apache MINA SSHD versions 2.0.0 to 2.19.0 and 3.0.0-M1 to 3.0.0-M5 for a certain (presumed rare) way to implement an SSH server. Apache MINA SSHD is a Java library for client- and server-side SSH. In the server part of the library, a mechanism to perform "asynchronous authentication" exists. A server implemented with Apache MINA SSHD must contain explicit code to make use of this feature. The implementation of this feature was flawed and could		

CVE-2026-77185	potentially lead to skipping checking the signature in public-key or hostbased authentication, or returning a wrong result. Users are recommended to upgrade to Apache MINA SSHD 2.20.0 or 3.0.0-M6, which fix the logic error and which additionally forbid the use of this "asynchronous authentication" mechanism with the public-key or hostbased authentication schemes: if used, the SSH session will be closed and the server will log an entry indicating that asynchronous authentication may be used only with password or keyboard-interactive authentication.	9.1	More Details
CVE-2026-97196	Improper Validation of Unsafe Equivalence in Input vulnerability in Liquid Web / StellarWP GiveWP allows Authentication Bypass. This issue affects GiveWP: from n/a through 4.16.9.	9.1	More Details
CVE-2026-76570	Joomla Extension - joomcode.com - Unauthenticated SQL injection in read and write queries in JCTables 1.21.1 - The front-end CRUD API controller performs no Joomla token validation and no authentication check on any task. Table names, column names, and values are taken directly from request parameters and concatenated into SQL queries, allowing SQLi for reading and writing queries.	9.1	More Details
CVE-2026-51859	bisheng 2.3.0, 2.4.0, and 2.4.0-beta1 is vulnerable to directory traversal in save_download_file (src/backend/bisheng/core/cache/utls.py:290).	9.1	More Details
CVE-2026-51864	DB-GPT v0.7.5 and v0.8.0 contains directory traversal in python_file_upload (packages/dbgpt-app/src/dbgpt_app/openapi/api_v1/python_upload_api.py:42). A remote attacker can use the validated exploitation path to write files outside the intended workspace or storage boundary.	9.1	More Details
CVE-2026-102794	A vulnerability has been found in Ziroom ZHOME A0101 1.0.1.0. This issue affects some unknown processing of the file /api/ZRnetwork/ping. Such manipulation of the argument url leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.1	More Details
CVE-2026-51883	The knowledge base creation and document upload interfaces in Langchain-Chatchat 0.3.0;0.3.1 is vulnerable to path traversal. An attacker can inject path traversal sequences (such as `..\`) into the `knowledge_base_name` parameter to write knowledge base content to arbitrary locations outside the configured knowledge base root directory.	9.1	More Details
CVE-2026-51879	deeptutor 1.4.0 contains an authorization bypass through a user-controlled object identifier in TutorBotManager.write_bot_file. A remote caller can enumerate bot IDs and overwrite another bot's whitelisted control files through the HTTP tutorbot file route.	9.1	More Details
CVE-2026-103648	Path traversal in image-downloader 4.3.0 allows an attacker who can control the download URL to cause downloaded response data to be written outside the configured destination directory.	9.1	More Details
CVE-2026-51876	DeepTutor 1.4.0 contains an authorization bypass vulnerability in the book confirmation flow. An unauthenticated or unauthorized caller can reuse a publicly exposed book_id to submit a confirm-proposal request for an existing book, causing unauthorized overwrites of persisted metadata and spine content.	9.1	More Details
CVE-2026-51875	In Devika v1.0, the Feature Agent save_code_to_project function contains a path traversal vulnerability that allows attackers to write files outside the intended project workspace, potentially compromising the entire server.	9.1	More Details
CVE-2026-56660	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. Prior to version 1.5, the update handler in UpdateCE.php downloads a ZIP archive and extracts its contents into the web root without validating file types or extraction paths. Because PHP files are written into a web-accessible directory, an attacker who can cause a malicious archive to be processed achieves remote code execution as the web-server user. Entry names are also used unsafely, allowing directory traversal (../) to write files outside the intended extraction directory. This issue has been patched in version 1.5.	9.1	More Details
CVE-2026-51906	In TaskingAI v0.3.0 in the DALL-E 3 image generation tool save_url_image function, a path traversal vulnerability allows attackers to write downloaded images to arbitrary locations on the server filesystem by manipulating the project_id parameter.	9.1	More Details
CVE-2026-53953	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. In version 3.3.22, the password reset endpoint can be accessed without authentication. When a reset request is submitted for an existing user, the application generates a new temporary password and immediately stores its hash as the user's new password. The temporary password is generated using PHP rand() seeded with microtime(). Because this seed is time-based and has a limited effective search space, an attacker can generate possible reset password candidates. Since the admin login endpoint does not enforce rate limiting or account lockout, these candidates can be tested online until the correct password is found. Successful	9.1	More Details

	exploitation may lead to administrator account takeover. At time of publication, there are no publicly available patches.		
CVE-2026-55083	DHIS2 is a flexible information system for data capture, management, validation, analytics and visualization. From versions 2.42.0 to before 2.42.5.1, and from versions 2.43.0 to before 2.43.0.1, DHIS2 is vulnerable to remote code execution (RCE) via unsafe Java deserialization. This issue has been patched in versions 2.42.5.1, 2.43.0.1, and 2.44.	9.1	More Details
CVE-2026-92084	The The Beaver Builder Page Builder – Drag and Drop Website Builder plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.11.0.5. 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. Exploitation requires the target site to have a Beaver Builder page containing the Sidebar module populated with a widget that displays attacker-controllable text, such as the core Recent Comments widget, with comment moderation disabled or the attacker's comment approved.	9.1	More Details
CVE-2026-102793	A flaw has been found in Ziroom ZHOME A0101 1.0.1.0. This vulnerability affects the function set_time_zone of the file /api/ZRFirmware/set_time_zone. This manipulation of the argument hostname/zonename causes command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.1	More Details
CVE-2026-96659	A flaw was found in Foreman. This vulnerability allows an authenticated user with low-level Viewer permissions to cause unauthorized information disclosure by submitting requests to template preview endpoints. By exploiting this issue, the user can access sensitive data, such as host root passwords. Furthermore, under insecure system configurations where Safemode protections are disabled, the flaw may allow the user to execute arbitrary commands as the Foreman system account.	9.1	More Details
CVE-2026-79898	Fortra BoKS Manager contains a command injection vulnerability in crlserver. An authenticated user authorized to add CRL URLs through BCC, the WSI REST or SOAP API, or the cacrl command-line interface could cause shell command substitution to be processed by crlserver as root on the BoKS Master. BCC and WSI provide network-accessible administration paths and do not require a local sudo or suexec rule; non-root use of cacrl requires such a rule.	9.1	More Details
CVE-2026-103264	Fleet versions before 4.87.0 contain an authentication bypass vulnerability in the device API that accepts hostnames and hardware serials as authentication tokens in addition to device UUIDs. Unauthenticated attackers who know or guess these non-secret identifiers can authenticate as iOS/iPadOS hosts to read device data and trigger device-scoped actions including software installation and MDM migration.	9.1	More Details
CVE-2026-92966	The The Appointment Booking Plugin – LatePoint Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.7.0. 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. The payload is planted during the unauthenticated booking flow and triggered when the Customer Cabinet block rendered by render_customer_dashboard() outputs the stored name into the content stream, where WordPress core's do_shortcode filter at priority 11 re-parses and executes it.	9.1	More Details
CVE-2026-92173	Prior to v74.0.0.878.1682 of Meta Horizon OS, MediaSyncJobReceiver could be induced to send a privileged PendingIntent including a com.oculus.vrshell CallerIdentity to an arbitrary application listening via NotificationListenerService. That would allow the application to impersonate the com.oculus.vrshell package, as well as packages signed with the same key, towards any endpoint within the OS that uses CallerIdentity authentication.	9.1	More Details
CVE-2026-87115	The VikAppointments Services Booking Calendar plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the extract function in all versions up to, and including, 1.2.21. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Exploitation requires at least one File-type custom field to be published on the confirmation page shortcode, as this field is not created by default during plugin installation.	9.1	More Details
CVE-2026-79820	A remote user validation failure vulnerability exists in HPE Integrated Lights-Out (iLO) 7 firmware.	9.0	More Details
CVE-2026-94389	Unauthenticated Remote Code Execution (RCE) in AcyMailing SMTP Newsletter <= 11.0.5 versions.	9.0	More Details
	OS command injection in the Studio Space startup validation script in Amazon SageMaker		

CVE-2026-104019	Distribution 2.x before 2.14.12, 3.x before 3.9.12, 4.0.x before 4.0.11, 4.1.x before 4.1.11, 4.2.x before 4.2.8, 4.3.x before 4.3.5, and 4.4.x before 4.4.3, as used by Amazon SageMaker Unified Studio, might allow an authenticated remote user with project contributor permissions to execute arbitrary commands in another project member's Studio Space and obtain that member's temporary execution role credentials via a crafted connection resource property that is interpolated into a shell invocation without neutralization. To remediate this issue, users should upgrade to version 2.14.12, 3.9.12, 4.0.11, 4.1.11, 4.2.8, 4.3.5, or 4.4.3, as applicable to the minor line in use. Users on minor lines that have reached end of support must move to a supported minor line, because no patched version will be released for those lines. In Amazon SageMaker Unified Studio, Studio Spaces adopt the latest patch of their minor line on restart once the patched images are deployed, so no version selection is required.	9.0	More Details
CVE-2026-103255	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a path traversal vulnerability in the Supabase node where the tableId parameter is inserted into request paths without validation. Attackers can exploit workflows binding tableId to untrusted input to traverse to Auth and Storage APIs using the administrative serviceRole key, bypassing Row Level Security and enabling unauthorized data access and modification.	9.0	More Details
CVE-2026-103248	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a filter injection vulnerability in the Supabase node's Filters (String) mode that fails to escape field values. Attackers can inject filter expressions from untrusted input to read all table rows, update all records, or delete entire tables in a single request.	9.0	More Details
CVE-2026-86345	A flaw was found in 389-ds-base. The server does not discard plaintext bytes already buffered from a client connection when negotiating StartTLS, allowing an on-path attacker to inject a crafted LDAP message that is processed after the TLS upgrade and whose response is delivered to the client in place of the client's own pending operation's response, due to messageID collision. This can cause a client application to treat a failed authentication (bind) attempt as successful.	9.0	More Details
CVE-2026-103056	AI SOC versions 7.2.0 before 12.0.0 contain a command injection vulnerability in the actions service that builds CrowdStrike Real Time Response command strings by interpolating unescaped action parameters in crowdstrike_rtr.py and endpoint.py. Authenticated users can inject single quotes into file_path, path, script_name, or script_args parameters to break out of quoted arguments and execute arbitrary commands on managed endpoints with SYSTEM or root privileges.	9.0	More Details
CVE-2026-55176	Soft Machine is a Virtual Machine-based agentic development environment / Cloud OS. In versions 0.2.247 and prior, two authentication helpers in /app/server.js — verifyContainerAuth() and authenticateWorkspaceHttp() — accept the global CONTAINER_SHARED_SECRET as a bearer token without verifying which workspace the caller belongs to. Because that secret is set identically on every container in the Fly app and is reachable from the user-facing process environment inside each workspace, any tenant can use it to authenticate to any other tenant's workspace API. The result is cross-workspace read, write, and destructive-restore primitives reachable from any paying customer's shell. The existing per-workspace token check (workspaceTokenMatches) protects the user-facing per-workspace token path, but the shared-secret bearer path bypasses it entirely. At time of publication, there are no publicly known patches.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-100277	In JetBrains YouTrack before 2026.2.19197 account takeover was possible by replaying a notification signature	8.9	More Details
CVE-2026-92931	CWE-918: Server-Side Request Forgery in the Progress @progress/sitefinity-nextjs-sdk npm package versions 15.1.8326 through 15.4.8637 may allow a remote attacker to make server-side requests to an attacker-controlled host, potentially exposing sensitive information.	8.8	More Details
CVE-2026-19807	The ByteCoreStack – MCP Connector for AI Tools plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2.3 This is due to the `wp_update_user_meta` MCP tool in `execute_tool` gating writes solely with `current_user_can('edit_user', \$uid)` — a check that WordPress core's `map_meta_cap` resolves to the `read` primitive when the target user ID matches the caller's own — while enforcing an incomplete meta key blacklist that covers only `user_pass`, `user_activation_key`, and `session_tokens`, leaving the `wp_capabilities` and `wp_user_level` meta keys entirely unprotected. This makes it possible for authenticated attackers with Subscriber-level access and above to elevate their privileges to Administrator by issuing a `wp_update_user_meta` call over the MCP JSON-RPC endpoint with `key=wp_capabilities` and an arbitrary role array such as	8.8	More Details

	`{'administrator': true}` targeting their own user ID, causing WordPress to load that account as an Administrator on the next request.		
CVE-2026-94678	Contributor PHP Object Injection in Go Live Update Urls <= 7.0.8 versions.	8.8	More Details
CVE-2026-20586	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS11383899; Issue ID: MSV-9614.	8.8	More Details
CVE-2026-94683	Contributor PHP Object Injection in DesignSetGo <= 2.8.0 versions.	8.8	More Details
CVE-2026-85573	The All in One Files Upload WordPress plugin before 2.0.17 adds SVG to the site's allowed upload types and does not sanitise uploaded files or verify the authenticity of its public upload requests, allowing unauthenticated users to store files containing active content which run in the site's origin when a victim opens them.	8.8	More Details
CVE-2026-95531	Subscriber PHP Object Injection in Conversational Forms for ChatBot <= 1.5.0 versions.	8.8	More Details
CVE-2026-103268	Ghost versions before 6.62.0 contain an authentication bypass vulnerability that allows suspended staff users to reactivate their accounts through self-service password reset. Attackers with suspended staff credentials can perform password reset operations to regain active account access and restore their original privileges.	8.8	More Details
CVE-2026-104851	fsspec is a specification and Python implementation framework for filesystem interfaces. From 0.9.0 until 2026.6.0, fsspec.implementations.reference.ReferenceFileSystem evaluates fields from Kerchunk reference JSON documents through unrestricted jinja2.Template(...).render(...) calls in _process_references1._render_jinja, _process_templates, and _process_gen in fsspec/implementations/reference.py. A document supplied inline or fetched from an attacker-controlled URL can provide template expressions that execute Python code when the reference filesystem is opened, including through consumers such as xarray, before referenced data is read. The _process_gen path is reached whenever a document includes a gen array, while the other paths depend on template-related options and values. This issue is fixed in version 2026.6.0.	8.8	More Details
CVE-2026-102377	Contributor PHP Object Injection in Photo Gallery by 10Web <= 1.8.46 versions.	8.8	More Details
CVE-2026-96451	Authorization Bypass Through User-Controlled Key vulnerability in Ultimate Member Ultimate Member ultimate-member allows Privilege Escalation.This issue affects Ultimate Member: from n/a through 2.13.1.	8.8	More Details
CVE-2026-59265	A code execution issue in the Java integration in Apache OpenOffice v4.1.16 and earlier allows a crafted untrusted document to trigger executing arbitrary (even remote) code when opened by the user. This issue is expected to be fixed in version 4.1.17, which is in the release candidate phase. Until then, users can mitigate this issue by disabling Java runtime integration in the Preferences dialog. This prevents the attack. If this is not possible, or as an extra precaution, you can avoid opening open untrusted files entirely. Once 4.1.17 is released, upgrade to that version to fix the issue.	8.8	More Details
CVE-2026-105123	W (vincent-peugnet/wcms) through 3.18.0 contains a remote code execution vulnerability that allows authenticated editors to write arbitrary files by abusing the unvalidated path in POST /api/v0/media/upload/[*:path]. Attackers can upload .php files executed by the web server, use encoded ../ sequences to write outside the media directory, and delete arbitrary files via DELETE /api/v0/media/[*:path].	8.8	More Details
CVE-2026-45524	In isSystem of WifiPermissionsUtil.java, there is a possible sandbox escape due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2026-103474	yii2-starter-kit through 4.2.0 fails to validate file types in the backend storage upload actions, allowing authenticated managers to upload PHP files. Attackers with manager role can upload PHP scripts to the web-accessible storage directory and request them to execute arbitrary code on the server.	8.8	More Details
CVE-	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in HAVELSAN Inc. Sef - AI Chatbot Platform allows SQL Injection. This issue affects Sef - AI Chatbot		More

2026-80298	Platform: before 2.1. NOTE: The vendor was contacted and it was learned that the product is not supported.	8.8	Details
CVE-2026-12405	A flaw was found in rubygem-foreman_remote_execution. A command injection vulnerability exists in the Red Hat Satellite API (/api/v2/job_invocations). When a job template has the effective_user property marked as overridable: true, the application fails to properly sanitize the effective_user input provided during the API request. The exploitation does not rely on the content or logic of the Job Template/playbook itself; rather, the injection occurs during the instantiation of the job execution environment by the Satellite server. An attacker with permissions to execute job templates can inject arbitrary shell commands into this parameter, which are executed on the target infrastructure with the privileges of the execution user.	8.8	More Details
CVE-2026-96837	Contributor Remote Code Execution (RCE) in CartFlows <= 3.2.0 versions.	8.8	More Details
CVE-2026-96838	Unauthenticated Cross Site Request Forgery (CSRF) in Blacklist Manager – WooCommerce Anti-Fraud, Blacklist & Checkout Verification <= 2.3.1 versions.	8.8	More Details
CVE-2026-95687	The WPC Shop as a Customer for WooCommerce plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.0.0 This is due to the plugin not properly validating the target user's role prior to issuing a new authentication session, allowing an authenticated attacker to log in as any WordPress Administrator by directly supplying an Administrator's user ID to the wpcsa_login endpoint and receiving a full Administrator session cookie without supplying the Administrator's password. This makes it possible for authenticated attackers to perform a direct session takeover, gaining full Administrator-level access to the site.	8.8	More Details
CVE-2026-51914	TransformerOptimus SuperAGI v0.0.14 is vulnerable to Incorrect Access Control in the agent template controller. In affected source snapshots, save_agent_as_template and publish_template in superagi/controllers/agent_template.py accept caller-supplied agent_id or agent_execution_id values and do not verify that the referenced agent or execution belongs to the authenticated user's organization.	8.8	More Details
CVE-2026-15897	The Super Forms – Drag & Drop Form Builder plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.3.316. This is due to the Register & Login add-on's before_email_success_msg() function, in its register_login_action='update' flow, trusting an attacker-supplied user_id value and passing it to wp_update_user() without any ownership or capability check. Because the super_save_form AJAX action also enforces no capability check, any authenticated user with Subscriber-level access and above can create the required malicious form (register_login_action='update' with register_login_user_id_update='true') and then submit it with user_id set to an administrator's ID along with a new user_pass/user_email. This makes it possible for authenticated attackers with Subscriber-level access and above to overwrite the credentials of arbitrary existing accounts — including administrators — resulting in account takeover and full site compromise.	8.8	More Details
CVE-2026-94121	Contributor PHP Object Injection in 10Web Booster – Website speed optimization, Cache & Page Speed optimizer <= 2.33.6 versions.	8.8	More Details
CVE-2026-18443	The Smart Manager – Advanced WooCommerce Bulk Edit & Inventory Management plugin for WordPress is vulnerable to generic SQL Injection via the 'access_privileges' parameter in all versions up to, and including, 8.97.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This exploit is only possible on installations where an administrator has saved a role-based deny-list Access Privilege configuration that does not explicitly block the internal 'access-privilege' module, as this condition allows the authorization filter to implicitly permit Subscriber-level users to invoke the vulnerable handler.	8.8	More Details
CVE-2026-55280	In multiple locations, there is a possible out-of-bounds write due to uninitialized data. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2026-51873	Devika v1.0 is vulnerable to Directory Traversal in the Coder.save_code_to_project function, which allows attackers to write files outside the intended project workspace.	8.8	More Details
CVE-2026-	In cfg2prop of btif_storage.cc, there is a possible out-of-bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User	8.8	More

58835	interaction is not needed for exploitation.		Details
CVE-2026-104714	Concurrent execution using shared resource with improper synchronization ('race condition') vulnerability in Apache Struts. Where a localized message formats a date or time argument, the formatter retained for that message by the application-wide text provider is used by concurrently served requests without isolation, so a value belonging to one user can appear in another user's response, or the rendering can fail and surface as a server error. Applications whose localized messages format no date or time arguments are not affected. This issue affects Apache Struts: from 2.0.0 through 2.3.37, from 2.5.0 through 2.5.33, from 6.0.0 through 6.11.0, from 7.0.0 through 7.3.0. Users are recommended to upgrade to version 6.12.0 or 7.4.0, which fixes the issue.	8.8	More Details
CVE-2026-103484	IVFFlat index build in pgvector before 0.8.7 allows a database user to write data out-of-bounds, which can lead to arbitrary code execution.	8.8	More Details
CVE-2026-94422	An incorrect implementation of message filtering in xdg-dbus-proxy versions before 0.1.9 allows an attacker to bypass the intended message filtering on the D-Bus session bus by setting a reply serial number on non-reply messages. A malicious or compromised Flatpak app could use this to achieve arbitrary code execution outside its sandbox. xdg-dbus-proxy was designed to be part of the sandbox boundary for Flatpak, but it is released as a separate project and is sometimes used by other app frameworks such as Firejail.	8.8	More Details
CVE-2026-103622	Use after free in SVG in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-103623	Use after free in MediaStream in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-88783	The Kubio AI Page Builder WordPress plugin before 2.9.3 does not limit its widening of the allowed HTML elements to the editor context, so the wider set is applied when filtering content submitted by unauthenticated users as well, allowing them to store markup which the Kubio AI Page Builder WordPress plugin before 2.9.3's own script later executes in the browser of any visitor, or of an administrator reviewing the still-unapproved submission.	8.8	More Details
CVE-2026-103625	Type confusion in V8 in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-104018	An improper privilege management vulnerability (CWE-269) exists in the command shell of Wind River VxWorks 7 when configured to enforce per-user command privileges. Under certain shell operations, a command may be evaluated without the privilege check that is normally applied, allowing an authenticated user with limited privileges to execute commands they are not authorized to run. Successful exploitation can result in privilege escalation, with impact to the confidentiality, integrity, and availability of the affected device. The issue affects all versions of VxWorks 7 prior to 26.09. It has been fixed in 26.09.	8.8	More Details
CVE-2026-103631	Buffer overflow in WebRTC in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-94076	Contributor PHP Object Injection in SEO Plugin by Squirrly SEO <= 14.2.5 versions.	8.8	More Details
CVE-2026-92994	The Verge3D Publishing and E-Commerce WordPress plugin before 4.13.1 does not validate the contents of files uploaded through its file storage feature and serves them back with an attacker-controlled content type, allowing unauthenticated attackers to store a file containing malicious JavaScript that executes in the browser of any user who opens it.	8.8	More Details
CVE-2026-93546	Integer overflow in mod_dav_fs in Apache HTTP Server through 2.4.68 allows an authenticated WebDAV client with write access to crash worker processes and persistently corrupt a directory's property database via PROPPATCH requests declaring many XML namespaces.	8.8	More Details
CVE-2026-100511	Deserialization of Untrusted Data vulnerability in Vektor Inc. VK Google Job Posting Manager vk-google-job-posting-manager allows Object Injection.This issue affects VK Google Job Posting Manager: from n/a through 1.3.1.	8.8	More Details

CVE-2026-103105	Pexip Infinity before 38.2, plus 39.0, 39.1 and 40.0, is affected by improper access control on a product-internal API which allows an attacker with local access to a node within a Pexip Infinity installation to execute arbitrary code as an unprivileged user on another Pexip Infinity node.	8.8	More Details
CVE-2026-96831	Contributor PHP Object Injection in Themify Builder <= 7.8.1 versions.	8.8	More Details
CVE-2026-105642	Ghost is a Node.js content management system. From 6.56.0 until 6.67.0, an image processing library bundled with Ghost contained a vulnerability in its SVG handling. Any staff user, including Contributors, could create a bookmark card for an attacker-controlled website, resulting in arbitrary commands being run on the Ghost server. This issue is fixed in version 6.67.0.	8.8	More Details
CVE-2026-92172	Prior to v66.0.0.733.524 of Meta Horizon OS, OVRMediaService could be induced to send a privileged PendingIntent including a com.oculus.horizon CallerIdentity to an arbitrary application registering for com.oculus.systemactivities.SCREENSHOT via a broadcast receiver. That would allow the application to impersonate the com.oculus.horizon package towards any endpoint within the OS that uses CallerIdentity authentication.	8.8	More Details
CVE-2026-102120	A privilege escalation vulnerability in Kiteworks could have allowed an attacker who had already obtained code execution on one node of a clustered Kiteworks deployment to run operating system commands with elevated privileges on another node of the same cluster. Insufficient input validation in an internal cluster management function let attacker-supplied values reach a privileged execution context; exploitation requires existing access to a node in the cluster, and the affected function is not reachable from outside the cluster.	8.8	More Details
CVE-2026-103068	Subscriber Privilege Escalation in ByteCoreStack – MCP Connector for AI Tools <= 1.2.2 versions.	8.8	More Details
CVE-2026-82039	UTMStack before 11.2.16 contains a SQL injection vulnerability in UtmAssetGroupService.searchQueryBuilder() that allows authenticated attackers to inject arbitrary SQL by supplying malicious assetType and groupName values that are inserted unsanitized into a native PostgreSQL query via String.format(). Attackers can exploit the GET /api/utm-asset-groups/searchGroupsByFilter endpoint to execute arbitrary SQL with DBA privileges, enabling full database read, data modification, and potential filesystem access.	8.8	More Details
CVE-2026-18783	Missing authentication for critical function vulnerability in Trex Digital Smart Manufacturing Systems Inc. Trex MES allows Authentication Bypass. This issue affects Trex MES: through 2026-09-29.	8.8	More Details
CVE-2026-39718	Cross-Site Request Forgery (CSRF) vulnerability in Webriti Wallstreet wallstreet allows Cross Site Request Forgery.This issue affects Wallstreet: from n/a through 2.8.6.	8.8	More Details
CVE-2026-92536	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.17.4 via the get_user_profile_structure. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract other users' email addresses, login names, and registration dates via the Member Directory's per-row user rebinding when attacker-controlled base64 payloads in the [pp-custom-html] shortcode invoke [profile-email], [profile-username], and [profile-date-registered]. When the WordPress users_can_register option is enabled, unauthenticated attackers can also exploit this vulnerability by supplying the split shortcode fragments through the plugin's own registration handler, which processes the reg_nickname and reg_bio fields without a nonce requirement.	8.8	More Details
CVE-2026-100253	In JetBrains TeamCity before 2026.2, 2026.1.4, 2025.11.8 sandbox escape leading to code execution was possible via the versioned settings Kotlin DSL	8.8	More Details
CVE-2026-100254	In JetBrains TeamCity before 2026.2, 2026.1.4, 2025.11.8 authenticated users could execute commands on Windows servers via CRLF injection in Pipeline Git connection settings	8.8	More Details
CVE-2026-97284	Contributor PHP Object Injection in Icegram <= 3.1.31 versions.	8.8	More Details
CVE-2026-	The CoCart WordPress plugin before 4.9.7 does not scope its REST API authentication filter to its own endpoints, which disables WordPress core's REST nonce protection for every route, allowing an attacker		More

93549	to perform a cross-site request forgery attack that creates a new administrator account using a logged-in administrator's session.	8.8	Details
CVE-2026-97644	The Groundhogg — CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to Privilege Escalation via Contact Identity Rebinding in all versions up to, and including, 4.9 The vulnerability exists because the `create_contact` function in the v3 REST endpoint (`POST /gh/v3/contacts`) is gated solely by the `add_contacts` capability and forwards the full request payload — including the security-bearing `user_id` column — into the upsert path of `Contacts_DB::add()`, which bypasses the ownership guard that `Contacts_DB::update()` enforces, allowing an attacker to rebind any existing contact record to an arbitrary WordPress user ID. This makes it possible for authenticated attackers with Sales Representative-level access and above to upsert their own contact row to point to an Administrator's user ID, then invoke the v4 email-test endpoint (`POST /gh/v4/emails/test`) — also accessible to the Sales Representative role via the `send_emails` capability — to generate an `{auto_login_url}` one-time permissions key bound to the rebound contact, and consume that link to call `wp_set_auth_cookie()` and gain a fully authenticated session as the WordPress Administrator.	8.8	More Details
CVE-2026-96940	Weak authorization in Microsoft Exchange Server allows an authenticated attacker to elevate privileges over a network.	8.8	More Details
CVE-2026-102125	The sandbox that isolates document conversion on a Kiteworks appliance did not fully confine the code running inside it. Code already executing within that sandbox could potentially escape its confinement and act with the privileges of the service account that runs the application, which could allow an attacker in that position to read or modify application data and configuration, or to disrupt the service on the affected appliance.	8.8	More Details
CVE-2026-97257	Deserialization of Untrusted Data vulnerability in PressTigers Simple Event Planner simple-event-planner allows Object Injection.This issue affects Simple Event Planner: from n/a through 1.5.7.	8.8	More Details
CVE-2026-101919	A flaw was found in the HyperShift operator. The operator copies user-provided Kubernetes configuration (kubconfig) secrets directly into the privileged control plane namespace without proper validation or sanitization. An authenticated user with cluster and secret creation permissions can exploit this vulnerability by supplying a configuration containing unauthorized executable plugins. When downstream controllers consume this configuration, an attacker can achieve arbitrary code execution within the control plane.	8.8	More Details
CVE-2026-80275	Comelit Multi-User Gateway for VIP System (model 1456B) firmware versions 2.9.1 and 2.10.0 fail to enforce server-side authorization on an administrative password-change function. An authenticated user level can invoke this function to overwrite the installer (administrator) account password.	8.8	More Details
CVE-2026-101882	OpenClaw Windows Node before 2026.7.1 contains an incomplete validation vulnerability in system.execApprovals.set that accepts wildcard-executable rules and abusable system binaries like mshta, rundll32, and certutil. Remote callers can add broad allow rules to execute arbitrary commands on the Windows host through system.run without operator checks or user prompts.	8.8	More Details
CVE-2026-66246	iControl is affected by a Broken Access Control vulnerability, which could allow an attacker to exploit missing authentication checks or insecure direct object references (IDOR), enabling privilege escalation and the unauthorized modification or deletion of sensitive application data.	8.8	More Details
CVE-2026-101880	OpenClaw Windows Node before 2026.7.1 contains an incorrect authorization vulnerability in the system.run exec-approval policy where ExecShellWrapperParser fails to split commands on pipe operators or extract command substitutions. Connected gateways or agents can bypass approval rules by placing denied commands behind allowed prefixes using pipe operators or command substitution syntax, achieving arbitrary command execution on Windows hosts.	8.8	More Details
CVE-2026-82828	Hitachi Coding Software Suite contains an Incorrect Authorization vulnerability that allows an unprivileged user to perform administrator-level operations. This issue affects Hitachi Coding Software Suite: through 3.3.0.	8.8	More Details
CVE-2026-101147	The Featured Image from URL (FIFU) WordPress plugin before 6.0.8, Featured Image from URL (FIFU) Premium WordPress plugin before 8.2.8 do not correctly enforce the REST API nonce, disabling the check for the whole request when a crafted URL is used, which could allow attackers to make a logged-in administrator perform any REST API action, such as creating a new administrator account, via a CSRF attack.	8.8	More Details
CVE-2026-	Contributor PHP Object Injection in Schema & Structured Data for WP & AMP <= 1.66 versions.	8.8	More

97291			Details
CVE-2026-105089	WWBN AVideo through 29.2.0 contains a stored cross-site scripting vulnerability that allows users with upload permission to inject script by setting a malicious video trailer1 URL. The value is rendered unescaped in YouPHPFlix2 templates and channel playlists, letting attackers break out of onclick strings or iframe src attributes to execute JavaScript in victims' browsers.	8.7	More Details
CVE-2026-55230	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to version 1.0.8.6, Vvweb's HTML sanitizer fails to strip event-handler attributes when a tag carries a greater-than character inside a quoted attribute value. A low-privilege content author (default role author or contributor) can store a payload in post or product content that runs JavaScript in a browser of every visitor and of any administrator who views or previews that content, which opens a path to admin account takeover. This issue has been patched in version 1.0.8.6.	8.7	More Details
CVE-2026-105630	Plane is an open-source project management tool. Prior to 1.4.0, an authenticated low-privilege workspace member, including a Guest, can upload an image/svg+xml file as a generic or issue attachment. The file retains the attacker-controlled Content-Type, and the asset-download endpoint creates a presigned URL with Content-Disposition: inline. In the default self-hosted MinIO deployment, the asset URL is served from the same origin as the Plane application, allowing embedded SVG JavaScript to execute in the application's security context. A victim, including a workspace administrator, who opens the link can have the session compromised through stored XSS, leading to account takeover. This issue is fixed in 1.4.0.	8.7	More Details
CVE-2026-19253	The Cache Enabler WordPress plugin before 1.8.17 does not validate a URL before using it to build a filesystem path in its cache purge routine, and does not confine the resulting deletion to the cache directory, allowing unauthenticated users to delete arbitrary files and directories on sites where another installed Cache Enabler WordPress plugin before 1.8.17 or passes a request-derived URL to its public cache-clearing hook.	8.7	More Details
CVE-2026-103253	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain an SQL injection vulnerability in the Oracle Database node's Delete Table Drop operation. Attackers can inject single quotes in the table or schema fields to append arbitrary SQL statements and execute DDL or DML commands against the connected database with the credential's privileges.	8.7	More Details
CVE-2026-102100	Kiteworks Core before version 9.5.0 is vulnerable to Stored Cross-Site Scripting. A stored cross-site scripting (XSS) weakness in Kiteworks Core could allow an authenticated user to submit content that, when later viewed by another user, executes arbitrary JavaScript in that user's authenticated session. This could be used to perform actions on the victim's behalf and may have permitted account takeover, including of higher-privileged users. Exploitation requires the victim to view the attacker-supplied content.	8.7	More Details
CVE-2026-105086	WWBN AVideo 12.4 through 29.2.0 contains a stored cross-site scripting vulnerability that allows authenticated uploaders to inject HTML by submitting doubly-encoded entities in video titles. Because safeString() strips tags before decoding entities and runs twice via setTitle() and save(), attackers can store markup that executes in trending, gallery, embed, and playlist pages.	8.7	More Details
CVE-2026-10764	Information disclosure in BVMS 4.5 up to 12.3 including allows man-in-the-middle attackers to gain unauthorized access to sensitive data.	8.7	More Details
CVE-2026-54049	Sakai is a Collaboration and Learning Environment (CLE). From versions 23.0 to before 23.5, and versions 25.0 to before 25.3, the Sakai Conversations tool stores topic and post messages without HTML sanitization, and the frontend renders them using LitElement's unsafeHTML() directive, resulting in stored cross-site scripting (XSS). Any authenticated user with access to a site that has the Conversations tool enabled can inject arbitrary HTML and JavaScript that executes in the browsers of all other users who view that topic or post. This issue has been patched in versions 23.5, 25.3, and 26.0.	8.7	More Details
CVE-2026-104979	Plane is an open-source project management tool. Prior to 1.4.0, IntakeIssuePublicViewSet.create in Plane v1.3.1 writes description_html through Issue.objects.create(...) without calling validate_html_content from nh3. Any authenticated user, including a new user with no workspace memberships, can plant arbitrary HTML in a project that has a published DeployBoard with intake enabled. When a project member or viewer of a closed intake item clicks the planted link, the TipTap \tjavascript: parser bypass and the target="_self" click handler execute JavaScript in the viewer's session and exfiltrate a long-lived API token. This issue is fixed in 1.4.0.	8.7	More Details
CVE-2026-102092	Kiteworks Core before version 9.5.0 is vulnerable to Stored Cross-site Scripting (XSS) that could allow an authenticated user to store crafted content that executes arbitrary JavaScript in another user's authenticated session when they preview shared content. This could potentially lead to session compromise and account takeover.	8.7	More Details

CVE-2026-104464	YesWiki before 4.6.7 contains a server-side request forgery vulnerability that allows unauthenticated attackers to make server-side GET requests by supplying an unvalidated actor URL to the Bazar abonnements sync action. Attackers can target internal hosts or cloud metadata endpoints and chain attacker-controlled outbox first/next links, with fetched responses stored as readable Bazar entries.	8.6	More Details
CVE-2026-89236	The SaveTo Wishlist Lite WordPress plugin before 1.1.5 does not sanitise and escape parameters before using them in the ORDER BY clause of a SQL query, allowing unauthenticated attackers to append additional SQL queries and extract sensitive information from the database.	8.6	More Details
CVE-2026-104457	YesWiki before 4.6.7 contains an SQL injection vulnerability in the Bazar filtertags action, which wraps unescaped filterN attribute tokens in quotes and concatenates them into a raw tags.value IN (...) clause. Unauthenticated attackers on default installs can save filtertags markup in a page with a trailing-backslash token that breaks quote parity under MySQL backslash escaping. This lets them inject a five-column UNION subquery to read arbitrary table data such as password hashes.	8.6	More Details
CVE-2026-103102	Pexip Infinity before 41.0 is affected by improper input validation in the signaling implementation which allows a remote attacker to trigger a software abort resulting in a denial of service. Exploitation of this issue requires accessing a gateway call from a WebRTC/API client.	8.6	More Details
CVE-2026-102121	A form-rendering interface in the Advanced Forms component is reachable without authentication so that published forms can be displayed to anonymous visitors, but it returned more data than the form itself required. Anyone who knew the web address of a published form could potentially retrieve the form owner's Kiteworks account profile, including personal details, along with parts of the deployment's configuration settings; no passwords, authentication tokens, or multi-factor secrets were exposed.	8.6	More Details
CVE-2026-103101	Pexip Infinity 30.0 through 40.x before 41.0 is affected by improper input validation in the web server that allows a malicious attacker to render a Pexip Infinity node inaccessible.	8.6	More Details
CVE-2026-89296	The Pro Like Button WordPress plugin before 2.0 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	8.6	More Details
CVE-2026-88789	Improper Restriction of XML External Entity Reference in the XSLT support extension (camel-quarkus-support-xalan) in Apache Camel Quarkus from 3.2.0 before 3.33.3 and from 3.34.0 before 3.40.0 on all platforms allows an attacker who supplies the XML document being transformed to read local files or issue requests to internal network locations via an external entity declaration in that document. The extension supplies its own Xalan-backed TransformerFactory to the xslt component and registers it as the JAXP default. Xalan-J 2.7.x predates JAXP 1.5 and does not honour javax.xml.XMLConstants.ACCESS_EXTERNAL_DTD or ACCESS_EXTERNAL_STYLESHEET, so the external access restrictions Apache Camel applies to the TransformerFactory it creates were not in effect. On the xslt component path this affects message bodies that reach the transformer already as a javax.xml.transform.Source; bodies of other types are converted to a SAXSource by Apache Camel with external entities and external DTD loading disabled, and are not affected. Because the factory is also the JAXP default, other code in the application obtaining one through TransformerFactory.newInstance() loses the same restrictions without error. Applications are affected if they use any of camel-quarkus-xslt, camel-quarkus-xslt-saxon, camel-quarkus-tika or camel-quarkus-xmlsecurity, each of which brings the XSLT support extension onto the classpath. For all but camel-quarkus-xslt, the exposure is limited to the JAXP default factory, since those extensions do not perform XSLT transformations themselves. Users are recommended to upgrade to version 3.33.3 or 3.40.0, which fixes this issue.	8.6	More Details
CVE-2026-105115	OpenAM before 16.1.3 contains an unauthenticated arbitrary class instantiation vulnerability in the legacy JAX-RPC SOAP interface that allows remote attackers to load classes without authentication. Attackers can send SOAP requests to /jaxrpc/* with an unverified session identifier and a chosen class name, crashing the server, probing the classpath, or potentially reaching code execution via gadget chains.	8.6	More Details
CVE-2026-95588	Unauthenticated Arbitrary File Deletion in AcyMailing SMTP Newsletter <= 11.0.5 versions.	8.6	More Details
CVE-2026-103066	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP BASE WP BASE Booking wp-base-booking-of-appointments-services-and-events allows Blind SQL Injection.This issue affects WP BASE Booking: from n/a through 6.4.0.	8.5	More Details
CVE-2026-94177	Unauthenticated SQL Injection in GamiPress <= 8.0.2 versions.	8.5	More Details

CVE-2026-103247	n8n versions before 1.123.80 contain a credential tampering vulnerability where duplicate node IDs bypass the workflow credential tamper guard. Attackers with editor access to shared workflows can exploit mismatched node ID and name matching to retain victim credentials and redirect secrets to attacker-controlled hosts.	8.5	More Details
CVE-2026-104389	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sirv Sirv sirv allows Blind SQL Injection.This issue affects Sirv: from n/a through 8.2.5.	8.5	More Details
CVE-2026-94115	Contributor SQL Injection in Easy Pricing Tables <= 4.1.2 versions.	8.5	More Details
CVE-2026-97293	Contributor SQL Injection in Media Library Assistant <= 3.41 versions.	8.5	More Details
CVE-2026-104971	Plane is an open-source project management tool. Prior to 1.4.0, DuplicateAssetEndpoint fetches a source FileAsset without limiting it to the caller's workspace, allowing cross-workspace asset duplication. WorkspaceFileAssetEndpoint and the legacy FileAssetEndpoint omit workspace authorization, allowing authenticated users to read, create, modify, or delete assets in workspaces where they are not members. Separately, WorkspaceViewViewSet.retrieve lacks the authorization decorator used by its sibling actions, exposing an unauthorized workspace-view read surface. This issue is fixed in 1.4.0.	8.5	More Details
CVE-2026-97287	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Blind SQL Injection.This issue affects Event Tickets: from n/a through 5.29.5.	8.5	More Details
CVE-2026-103338	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Blind SQL Injection.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.20.	8.5	More Details
CVE-2026-102379	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VillaTheme BuildKit - Product Builder for WooCommerce - Custom PC Builder woo-product-builder allows Blind SQL Injection.This issue affects BuildKit - Product Builder for WooCommerce - Custom PC Builder: from n/a through 1.0.28.	8.5	More Details
CVE-2026-94591	Armatura One stores database and message-broker credentials in an install configuration file, encrypting them with AES-128-CBC when this protection is enabled. The encryption key and initialization vector are fixed values embedded in the software itself and are identical across every installation. An attacker with a copy of the installation package can recover this key and initialization vector, and can then decrypt the stored credentials of any specific installation to which the attacker separately obtains the encrypted configuration file.	8.4	More Details
CVE-2026-19184	The NXP GAU ADC driver (drivers/adc/adc_mcux_gau_adc.c) validated the caller-supplied sequence->buffer_size, which is expressed in bytes, against the number of active channels, which is a sample count. It then stored that byte count directly in data->results_length and used it in mcux_gau_adc_read_samples() as the number of uint16_t slots available. Because each conversion result occupies sizeof(uint16_t) bytes, a buffer that was accepted as "large enough" could be written with up to twice its size in bytes, so every sample past the buffer's midpoint was written out of bounds. adc_read() and adc_read_async() are Zephyr system calls. The syscall verifier in drivers/adc/adc_handlers.c only confirms that the caller owns buffer_size writable bytes (K_SYSCALL_MEMORY_WRITE); deciding whether that size is sufficient for the requested channels and extra_samplings is delegated entirely to the driver. On a build with CONFIG_USERSPACE=y, a user-mode thread that has been granted the ADC device object could therefore submit a deliberately half-sized buffer and cause the driver's work-queue handler — which runs in supervisor mode, outside the caller's MPU restrictions — to write ADC conversion results past the end of that buffer, at an address and for a length of the caller's choosing. The overrun is bounded by the requested sequence: with sequence->options->extra_samplings set, the sampling loop walks the buffer pointer forward across every sampling, so the total overrun can reach the full size of the supplied buffer (kilobytes for a large extra_samplings). The written words are 16-bit ADC conversion results, so the content is only partially attacker-influenced (via the selected analog input, gain and resolution), but the destination and length are fully controlled — sufficient for kernel memory corruption, a crash, or a userspace-to-kernel privilege escalation. Builds without CONFIG_USERSPACE, or on SoCs other than NXP RW61x with the GAU ADC node enabled, are not exposed to the privilege boundary; there the same defect only causes a silent overflow when the application itself passes an undersized buffer. The fix replaces the ad-hoc check with the shared adc_sequence_validate_buffer() helper (validating against num_channels * 	8.4	More Details

	sizeof(uint16_t)), stores buffer_size / sizeof(uint16_t) in results_length, and corrects the loop bound to a post-decrement so exactly the available number of slots may be written.		
CVE-2026-94592	Armatura One's database initialization routine assigns a fixed, vendor-defined password to the database superuser account at creation time, rather than generating a unique password per installation. An individual with access to the server operating system and knowledge of this value can authenticate as the database superuser on a deployment where it has not been changed.	8.4	More Details
CVE-2026-20523	In neuropilot, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11249062; Issue ID: MSV-9171.	8.4	More Details
CVE-2026-20522	In neuropilot, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11249050; Issue ID: MSV-9172.	8.4	More Details
CVE-2026-20531	In apu, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11249016; Issue ID: MSV-9169.	8.4	More Details
CVE-2026-20521	In Video HAL, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11375674; Issue ID: MSV-9571.	8.4	More Details
CVE-2026-20524	In apu, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11249004; Issue ID: MSV-9170.	8.4	More Details
CVE-2026-46711	Soft Machine is a Virtual Machine-based agentic development environment / Cloud OS. In versions 0.2.247 and prior, the workspace HTTP service that listens on 0.0.0.0:8080 inside each sm-ws-* Fly Machine exposes endpoints (/health, /file/<path>, /archive/<dir>) without any authentication or origin check. Any host that can reach TCP/8080 on a workspace can read arbitrary files under that workspace's /workspace root and download whole project trees as tar archives. Because every workspace shares the same Fly private 6PN and resolves all peer addresses via the unauthenticated _instances.internal TXT record, every other sm-ws-* machine on the same Fly app/org is a reachable, unauthenticated attacker — the trust boundary (workspace owner ↔ everyone-else) is missing. At time of publication, there are no publicly known patches.	8.3	More Details
CVE-2026-102667	Joyland AI app allows an attacker with shared network access to inject JavaScript into content loaded in WebView. Without user-granted permissions, an attacker could access the clipboard, make arbitrary HTTP requests via the Weex 'stream' module, or access app-internal storage. If the installed app has been granted permissions previously, the attacker can access the entire file system, camera, microphone, and GPS tracking.	8.3	More Details
CVE-2026-103624	Use after free in Contextual Tasks in Google Chrome on on Windows prior to 154.0.8037.97 allowed a remote attacker who had compromised the renderer process to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-105213	ZITADEL 4.x before 4.17.1 does not check an organization's inactive state during Login V2 authentication, verifying only the individual user's status. Users of a deactivated organization who hold valid credentials, an existing session, or a refresh token can still sign in, create sessions, and obtain or refresh tokens.	8.2	More Details
CVE-2026-12541	A flaw was found in Foreman. OS command injection vulnerabilities exist in the foreman-rake db:dump and db:import_dump tasks. The application fails to properly sanitize user-supplied input in the destination parameter (during backups) and the file parameter (during imports) before passing them to a Ruby system() call for execution. An attacker with permissions to execute foreman-rake (e.g., via a restricted sudo configuration) can append malicious shell commands to the provided file paths.	8.2	More Details
CVE-2026-104978	Plane is an open-source project management tool. Prior to 1.4.0, Plane's project invitation list endpoint is accessible to any authenticated user who knows the workspace slug and project ID, while the public project invitation join endpoint accepts an invitation based only on a submitted email address. When a pending invitation targets an email address that has not registered with Plane, an attacker can enumerate the invitation, register an account using the invited email without mailbox verification, and accept the invitation. The attacker-controlled account is then added to the target workspace and project. This issue is fixed in 1.4.0.	8.2	More Details
CVE-2026-93621	Unauthenticated SQL Injection in WP Data Access <= 5.5.84 versions.	8.2	More Details

CVE-2026-91078	The TillKit WordPress plugin before 1.0.5 does not require the hard-coded, publicly known PIN of the privileged POS account it creates on activation to be changed before use, and it authenticates its public POS login endpoint on that PIN alone with no identity or capability check, allowing unauthenticated attackers to obtain a privileged POS session and thereby read customer and site-user personal data and modify store data.	8.2	More Details
CVE-2026-104051	PictShare before 3.7.1 contains an information disclosure vulnerability that allows unauthenticated attackers to obtain the secret delete_code and uploader metadata by calling the API::info() endpoint which returns the complete raw metadata object without a field whitelist. Attackers can use the publicly visible file hash to retrieve the delete_code via the info API and then invoke the delete API to permanently delete arbitrary files, while also exposing uploader IP, User Agent, remote port, and SHA-1 hash, resulting in loss of content integrity, availability, and uploader privacy.	8.2	More Details
CVE-2026-104445	YesWiki before 4.6.7 contains an authentication bypass vulnerability in the ActivityPub inbox that fails to bind the verified HTTP signature signer to the activity actor. Unauthenticated attackers with any ActivityPub keypair can send signed Delete or Update activities referencing a mirrored entry's sourceUrl to delete or overwrite other actors' federated entries.	8.2	More Details
CVE-2026-97662	An argument injection issue in the diff scan operation in AWS security-agent-mcp-server before version 0.2.0 might allow context-dependent threat actors to create, overwrite, or truncate arbitrary files on the host outside the intended workspace directory via a crafted reference value supplied to the diff scan operation. To remediate this issue, users should upgrade to version 0.2.0.	8.2	More Details
CVE-2026-96817	Subscriber Broken Access Control in MakeCommerce for WooCommerce <= 4.1.0 versions.	8.2	More Details
CVE-2026-12540	A flaw was found in Foreman. A command injection vulnerability exists in the foreman-rake errors:fetch_log task. The request_id parameter is passed to an underlying system command (typically grep) without adequate shell neutralization. While the task is intended to fetch specific log entries, an attacker with sudo permissions to execute this rake task can inject shell metacharacters (such as ;, ", or) to break out of the intended command and execute arbitrary code.	8.2	More Details
CVE-2026-100273	In JetBrains YouTrack before 2026.2.19197 authorisation bypass in the scripts debugger allowed arbitrary code execution	8.2	More Details
CVE-2026-103065	Improper Validation of Specified Quantity in Input vulnerability in Themeum Kirki kirki allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Kirki: from n/a through 6.3.1.	8.2	More Details
CVE-2026-105210	ZITADEL 3.x before 3.4.15 and 4.x before 4.17.1 contains a missing authentication flaw in the hosted Login V1 UI, whose second-factor enrollment and initialization handlers act on an identify-only session before any primary factor is verified. Attackers knowing only a victim's login name can enroll attacker-controlled TOTP, OTP-SMS, OTP-Email, or U2F factors, overwrite the verified phone number, and enumerate users through discrepant errors.	8.2	More Details
CVE-2026-103758	Obot 0.21.1 through 0.24.1 contains an authorization bypass vulnerability that allows authenticated users to reach MCP servers because the checkUI deny list omits the /mcp-connect-composite/ route. Basic-role users with a composite MCP ID can proxy requests through mcpGateway.Proxy to invoke tools on MCP servers restricted by Access Control Rules.	8.1	More Details
CVE-2026-105650	Ghost is a Node.js content management system. From 2.1.0 until 6.64.0, embedding a URL from an attacker-controlled website could result in untrusted scripts being stored in post content. These scripts could run in the Ghost editor, on the published site, and in newsletter emails, possibly resulting in compromise of a staff user's admin session. This issue is fixed in version 6.64.0.	8.1	More Details
CVE-2026-14316	The revoked-key error path builds a human-readable failure reason using sprintf() into a heap buffer. The allocated buffer is too small for the final formatted message. When sprintf() writes the full message, it can write past the end of the heap allocation.	8.1	More Details
CVE-2026-51901	SuperAGI up to 0.0.14 is vulnerable to Incorrect Access Control. The agent execution controller endpoint /api/agentexecutions/schedule allows authenticated users from one organization to schedule existing agents belonging to a different organization without proper authorization checks. The endpoint accepts an agent_id parameter but does not verify that the agent belongs to the authenticated user's organization.	8.1	More Details
	Tugtainer is a self-hosted app for automating updates of Docker containers. Prior to version 1.31.3, when the OIDC login flow completes, backend/modules/auth/providers/auth_oidc_provider.py decodes		

CVE-2026-87004	the id_token returned by the identity provider's token endpoint using jose.jwt.get_unverified_claims() instead of jwt.decode(). This skips signature verification, audience (aud) validation, issuer (iss) validation, and expiry (exp) checking entirely. The extracted claims (email/sub/preferred_username) are then used directly as the user_id for the resulting Tugtainer session. This issue has been patched in version 1.31.3.	8.1	More Details
CVE-2026-104059	Lektor 3.3.14 and 3.4.0b15 contains a cross-site request forgery vulnerability in the admin API blueprint that allows unauthenticated attackers to perform state-changing actions by sending cross-origin requests without CSRF tokens, Origin/Referer validation, CORS configuration, or Host allowlisting. Attackers can exploit the newattachment, deleterecord, build, clean, and publish endpoints from a malicious web page to write arbitrary files, delete pages, wipe build output, trigger deployment publication, and via DNS rebinding reach read endpoints to disclose data.	8.1	More Details
CVE-2026-104905	FacturaScripts before version 2026.7 contains a PHP object injection vulnerability in WidgetSelect::processFormData() that allows authenticated attackers to trigger unserialize() on raw POST data without an allowed_classes filter for multiple-select fields. Attackers can submit a serialized XLSXWriter object as the field value to invoke its __destruct() method, deleting arbitrary attacker-specified files such as config.php or backup data, resulting in denial of service and potential application reinstall hijack.	8.1	More Details
CVE-2026-104467	YesWiki before 4.6.7 contains an authorization bypass vulnerability in ApiService::isAuthorized() that allows unauthenticated attackers to call admin-only API routes when public API mode is enabled. Attackers can send requests to endpoints like api/ci/update_config and api/archives to overwrite configuration and list, download, or delete backup archives.	8.1	More Details
CVE-2026-103493	In JetBrains YouTrack before 2026.2.19422 stored XSS via Mermaid and LaTeX content was possible	8.1	More Details
CVE-2026-104414	Ghost from 2.5.0 before 6.64.0 contains a stored cross-site scripting vulnerability that allows attackers to inject untrusted scripts into post content via oEmbed photo responses. Attackers can host malicious oEmbed photo responses so that embedding their URL stores scripts that run in the Ghost editor, published site, and newsletter emails, compromising staff admin sessions.	8.1	More Details
CVE-2026-103250	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a NoSQL injection vulnerability in the MongoDB Chat Memory node that fails to validate the sessionId parameter. Unauthenticated attackers can supply MongoDB query operators in the sessionId field to access conversation histories from other users and perform unauthorized write and delete operations.	8.1	More Details
CVE-2026-103283	Ghost versions 6.20.0 before 6.57.1 contain a session handling vulnerability that allows authenticated staff users to log in as any other staff user with only the password, bypassing two-factor authentication. Attackers with valid staff credentials can exploit improper session management to impersonate other staff members and gain unauthorized access to administrative functions.	8.1	More Details
CVE-2026-101923	The Photo Reviews for WooCommerce plugin for WordPress is vulnerable to Arbitrary Content Deletion in versions up to, and including, 1.2.30. This is due to the plugin storing attacker-controlled post IDs from the wcpr_image_upload_id parameter of a public review submission into the review's reviews-images comment meta without verifying that the IDs correspond to attachments owned by the submitter, combined with the delete_reviews_image() handler unconditionally calling wp_delete_post(\$id, true) on every stored ID when the review is deleted. This makes it possible for unauthenticated attackers to permanently delete arbitrary posts, pages, products, or media attachments on the site whenever an administrator subsequently deletes the attacker's review (or when WordPress's built-in wp_scheduled_delete cron empties the comment trash after 30 days).	8.1	More Details
CVE-2026-103432	apcupsd through 3.14.14 has an sscanf stack-based buffer overflow in getupsvar() in src/cgi/upsfetch.c (used by upsstats.cgi, multimon.cgi, and upsfstats.cgi), a related issue to CVE-2026-15544.	8.1	More Details
CVE-2026-103277	Ghost versions from 2.5.0 before 6.34.0 contain an untrusted script execution vulnerability in the oEmbed preview feature that fails to sandbox externally hosted scripts. Attackers can craft malicious oEmbed content to execute scripts in the context of a staff user's admin session, potentially compromising administrative access.	8.1	More Details
CVE-2026-103473	Deno versions 2.7.0 through 2.9.7 on Windows contain a command injection vulnerability in node:child_process where shell arguments are escaped for the wrong shell type. Attackers can inject OS commands by passing untrusted arguments with the shell option, allowing arbitrary command execution with Deno process privileges.	8.1	More Details
	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to arbitrary file operations in all		

CVE-2026-92820	versions up to, and including, 3.3.34 via the external (Amazon S3) upload flow. The plugin trusts an attacker-supplied file path from the form submission and stores it as the upload's file_path, which is then used without validation to attach a file to the form's notification email (arbitrary file read), to write fetched content (arbitrary file write, leading to remote code execution when the external store is configured), and in a scheduled deletion (arbitrary file deletion). This makes it possible for unauthenticated attackers to read, write, or delete arbitrary files on the server. Exploitation requires the site to use the plugin's External File Upload (Amazon S3) action; the read variant additionally requires a form Email action configured to attach the uploaded file.	8.1	More Details
CVE-2026-73636	Authentication bypass by capture-replay in mod_auth_digest in Apache Software Foundation Apache HTTP Server 2.4.x on all platforms allows a man-in-the-middle (MITM) attacker to replay captured digest authentication credentials via crafted requests that trigger garbage collection of the client's shared memory entry when AuthDigestNonceLifetime is set to 0. Users are recommended to upgrade to version 2.4.69, which fixes this issue.	8.1	More Details
CVE-2026-104974	Plane is an open-source project management tool. Prior to 1.4.0, a user whose account has been deactivated by setting is_active=False can still log in with existing credentials. Successful authentication silently changes is_active back to True, reactivating the account without notifying the administrator. This issue is fixed in 1.4.0.	8.1	More Details
CVE-2026-51570	modelscope Agentscope v1.0.0-v1.0.8 is vulnerable to Path Traversal in insert_text_file.	8.1	More Details
CVE-2026-104443	YesWiki before 4.6.7 contains an empty-filter scope bypass in the triples delete API that allows any authenticated user to delete or forge arbitrary semantic triples regardless of ownership. Attackers can send an empty filter to the triples delete endpoint to remove the admins-group membership triple, emptying the admin group and causing a site-wide authorization lockout.	8.1	More Details
CVE-2026-51907	In TaskingAI v0.3.0 in the QR Code Generator plugin save_base64_image function, a path traversal vulnerability allows attackers to write image files to arbitrary locations on the server filesystem by manipulating the project_id parameter.	8.1	More Details
CVE-2026-103398	OpenSave through 2.4.0 fails to properly validate save paths supplied by paired peers in the manifest request handler. Attackers can specify arbitrary directories outside configured save locations to read and write files through manifest and sync routes.	8.1	More Details
CVE-2026-86136	A missing authorization vulnerability in the wagent management daemon's session initialization function allows an authenticated, low-privileged user (including a read-only or guest administrator account) to crash the wagent process and read arbitrary files accessible to the daemon by submitting a specially crafted management API request.	8.1	More Details
CVE-2026-90441	A missing authorization vulnerability in the wagent management daemon's session initialization function allows an authenticated, low-privileged user (including a read-only or guest administrator account) to crash the wagent process and read arbitrary files accessible to the daemon by submitting a specially crafted management API request.	8.1	More Details
CVE-2026-105211	ZITADEL before 4.17.1 contains an authentication bypass vulnerability in Login V2 that allows unauthenticated attackers to take over accounts by obtaining OTP codes via the returnCode delivery type. Attackers knowing a login name of a victim with OTP-Email and OTP-SMS enrolled can read both codes from server-action responses to gain MFA-authenticated sessions, including administrator takeover.	8.1	More Details
CVE-2026-102101	Kiteworks Core before version 9.5.0 is vulnerable to Deserialization of Untrusted Data. A deserialization weakness in Kiteworks Core could, under certain conditions, allow crafted data to be deserialized unsafely, potentially resulting in remote code execution on the appliance. Exploitation depends on an attacker first being able to influence the affected data, so this issue is not exploitable on its own.	8.1	More Details
CVE-2026-104988	A flaw was found in Dogtag PKI (pki-core). The CMCAuthForEST authentication plugin fails open when an EST fullcmc enrollment request is submitted via BasicAuth without an end-user TLS client certificate. The SSL_CLIENT_CERT session attribute retains the EST subsystem's agent certificate, which causes downstream authorization checks to treat the request as agent-privileged. An authenticated EST user can exploit this to obtain CA-signed certificates with arbitrary subject names.	8.1	More Details
CVE-	The Super Forms - Drag & Drop Form Builder plugin for WordPress is vulnerable to Arbitrary File/Directory Deletion in all versions up to, and including, 6.3.316. This is due to the `super_save_form` AJAX handler performing no capability check — allowing Subscriber-level authenticated users to create or modify Super Forms and enable the `file_upload_submission_delete` setting — combined with the `super_submit_form` handler's `submit_form` function passing the attacker-controlled `files[].subdir` value from `\$_POST['data']` directly into `SUPER_Common::delete_dir()` without sanitization, and a		

2026-15983	trivially bypassed `ABSPATH` guard that a `subdir` value of `wp-config.php` defeats because `dirname(realpath(ABSPATH . \$subdir))` resolves to the WordPress root while the naive `ABSPATH !== \$dir` string check fails to match due to a trailing-slash mismatch. This makes it possible for authenticated attackers, with Subscriber-level access and above, to recursively delete arbitrary files and directories on the server, up to and including the entire WordPress installation, resulting in full site takedown and potential remote code execution if critical files such as `wp-config.php` are removed and the site is subsequently re-installed by another party.	8.1	More Details
CVE-2026-105634	Plane is an open-source project management tool. Prior to 1.3.0, the ProjectMemberViewSet.partial_update method allows any project member, including a user with the lowest GUEST role, to modify another project member's role. The authorization check prevents assigning a role higher than the requester's role but does not prevent assigning a lower or equal role, allowing a Guest to demote Administrators and Members and deny them project control. This vulnerability is fixed in 1.3.0.	8.1	More Details
CVE-2026-104448	YesWiki before 4.6.7 contains a cross-site request forgery vulnerability in the ajaxdeletepage handler, which permanently deletes a page on any GET request carrying a jsonp_callback parameter without checking a CSRF token. Attackers can lure a logged-in administrator or page owner to a crafted link to delete arbitrary pages along with their ACLs, links, triples, comments and referrers.	8.1	More Details
CVE-2026-104970	Plane is an open-source project management tool. From 0.13 until 1.4.0, InstanceAdminSignUpEndpoint in apps/api/plane/license/api/views/admin.py:89-117, 173-229 uses InstanceAdmin.objects.first() for the first-admin check and performs account creation without an atomic transaction, row lock, uniqueness guard, or advisory lock. Two concurrent unauthenticated requests with different email addresses can both observe that no instance administrator exists, create separate User and InstanceAdmin rows, and receive sessions with instance-admin authority. This allows an attacker to share unrestricted instance administration with the legitimate operator. This issue is fixed in 1.4.0.	8.1	More Details
CVE-2026-51568	modelscope Agentscope v1.0.18-v1.0.0 is vulnerable to Path Traversal in write_text_file.	8.1	More Details
CVE-2026-105293	Legcord 1.1.0 through 1.3.0 contains a path traversal vulnerability in theme IPC handlers that allows script in the Discord page to escape the themes directory via unvalidated theme ids. Attackers running script in the Discord origin, such as through XSS, can abuse themes.folder, themes.uninstall, and themes.install to launch local executables, recursively delete directories, and write files outside the themes directory.	8.1	More Details
CVE-2026-100255	In JetBrains TeamCity before 2026.2, 2026.1.4, 2025.11.8 administrator account takeover was possible via password reset	8.1	More Details
CVE-2026-79625	Affected products do not properly synchronize access to their monitoring functionality. When multiple clients send concurrent requests, this may lead to incorrect reads or writes, or to corruption of internal memory structures. An authenticated remote attacker with monitoring access can exploit this issue to cause incorrect data processing or a denial-of-service condition.	8.1	More Details
CVE-2026-93994	Apache MINA SSHD is a Java library for client-side and server-side SSH. SSH servers can be configured to require multi-authentication schemes, for instance two different public keys, not just one. In OpenSSH, this would be done by setting in sshd_config AuthenticationMethods "publickey,publickey". Apache MINA SSHD provides an equivalent configuration mechanism. In Apache MINA SSHD versions up to 2.19.0 and 3.0.0-M1 to 3.0.0-M5 the server code in component sshd-core does not enforce that the two public keys presented are different. A user can thus successfully authenticate with only one of the two key pairs required by presenting this single key twice. This is a partial authentication bypass. Users are recommended to upgrade to version 2.20.0 or 3.0.0-M6, which fix this issue.	8.1	More Details
CVE-2026-94505	The Nelio Content – Editorial Calendar & Social Media Auto-Posting plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.5.0 This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to permanently delete any reusable social message (nc_reusable_social post), including those authored by administrators or other privileged users.	8.1	More Details
CVE-2026-102126	A stored cross-site scripting (XSS) weakness in Kiteworks Core could allow an administrator holding only a single, narrowly scoped delegated permission to store crafted content that later executes arbitrary JavaScript in the authenticated session of a System Administrator who views the affected page. This could have permitted the lower-privileged administrator to escalate to full administrative control of the tenant, including the creation of a new administrative account.	8.1	More Details
CVE-	Cross-Site Request Forgery (CSRF) vulnerability in Memberful Memberful - Membership Plugin		

2026-103067	memberful-wp allows Cross Site Request Forgery.This issue affects Memberful - Membership Plugin: from n/a through 1.81.0.	8.0	More Details
CVE-2026-103292	Ghost versions from 0.5.3 through versions prior to 6.50.0 fail to sanitize the data placed in the JSON-LD HTML tag emitted by the {{ghost_head}} helper. An authenticated user with limited privileges can inject unescaped content that is rendered as script in the published page, potentially leading to compromise of a staff user's admin session when that user views the affected page.	8.0	More Details
CVE-2026-79899	Fortra BoKS Manager contains an insecure temporary file vulnerability in bccgethostcert. The utility creates predictable temporary files without first setting a restrictive umask. A local user on the BoKS Master who can read files under BOKS_tmp may be able to obtain CA secret or host private-key material while the utility runs, or obtain CA secret material left behind after successful certificate creation.	7.9	More Details
CVE-2026-77805	In Progress® Telerik® Fiddler® Classic for Windows, versions prior to v6.0.20262.10021, the integrity check applied to the external helper tools launched by the application is insufficient. Before executing a helper tool, the application only verifies that the file carries a valid Authenticode signature whose certificate subject name matches a broad allow list of publisher name fragments, rather than verifying that the file is the specific executable shipped with that version of the product. A local threat actor with low privileges who replaces one of these helper executables with any other validly signed binary from an allow-listed publisher can cause the substituted binary to be executed by the application, including with Administrator privileges for the tools that request elevation, resulting in privilege escalation and execution of unintended code. Successful exploitation requires the user to launch the affected external tool and to approve the elevation prompt without noticing that it refers to a different executable.	7.9	More Details
CVE-2026-47510	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an integer overflow leading to an out-of-bounds write to GPU memory. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47502	NVIDIA vGPU Virtual GPU Manager for Windows and Linux contains a vulnerability in the kernel mode layer, where a guest user could cause an integer overflow leading to memory corruption. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47503	NVIDIA GPU Display Driver for Linux contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a guest VM user may cause an out-of-bounds write by sending a crafted RPC message with invalid performance state list size parameters. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47500	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where improper cleanup of reference counts during error paths could lead to a use-after-free condition. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47504	NVIDIA Linux GPU Display Driver contains a vulnerability in the NGX updater where an outdated embedded cryptographic library is susceptible to type confusion. A successful exploit of this vulnerability might lead to code execution, denial of service, information disclosure, or data tampering.	7.8	More Details
CVE-2026-47505	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer where an attacker could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, denial of service, or escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47507	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an out-of-bounds array access. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47508	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an incorrect conversion between numeric types. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47501	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a user could cause an out-of-bounds write by supplying mismatched memory buffers during event buffer setup. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-	NVIDIA GPU Display Driver for Windows contains a vulnerability in the display driver DIAG escape handler where a local unprivileged attacker may cause an integer overflow and out-of-bounds write. A		More

47575	successful exploit of this vulnerability might lead to denial of service, and code execution.	7.8	Details
CVE-2026-47499	NVIDIA vGPU Virtual GPU Manager for Windows and Linux contains a vulnerability in the kernel mode layer where a guest could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47498	NVIDIA vGPU Manager contains a vulnerability in the GPU System Processor (GSP) plugin where a guest VM user may cause an out-of-bounds write by sending a specially crafted RPC message. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-94593	Armatura One's backup and restore routine records the full database connection command, including the superuser password, in plain text in a log file on the host. Credentials disclosed by this finding can be used to access the database when access to the server operating system is available.	7.8	More Details
CVE-2026-105220	Twine 2 desktop through 2.12.0 contains a cross-site scripting vulnerability in importStories() that executes markup from imported story files in the editor window. Attackers can craft a story file whose script calls the twineElectron openWithScratchFile IPC bridge to write and open a .bat file, executing code as the user.	7.8	More Details
CVE-2026-102118	A local privilege escalation vulnerability in Kiteworks could have allowed an attacker with an existing shell under a low-privileged service account to escalate to root privileges on the appliance.	7.8	More Details
CVE-2026-102113	A privilege escalation vulnerability in Kiteworks could allow an attacker who has already obtained code execution as an unprivileged backend service account on the appliance to escalate to root. A privileged routine did not safely handle a filesystem path that the lower-privileged account could influence, allowing the attacker to cause a root-owned operation to run arbitrary commands with the highest privileges. Exploitation requires existing local access to that service account.	7.8	More Details
CVE-2026-102112	A privilege escalation vulnerability in Kiteworks could allow an attacker who has already obtained code execution as an unprivileged backend service account on the appliance to escalate to root and run arbitrary commands with the highest privileges. Exploitation requires existing local access to that service account.	7.8	More Details
CVE-2026-78860	An issue in Mercusys AC12 V2 allows a local attacker to execute arbitrary code via the storage of information in plaintext	7.8	More Details
CVE-2026-100256	In JetBrains IntelliJ IDEA before 2026.2.3 rCE via Structural Search script constraints was possible in untrusted projects	7.8	More Details
CVE-2026-19185	The system-call verifier for i3c_do_ccc() in drivers/i3c/i3c_handlers.c validated the outer struct i3c_ccc_payload, the broadcast ccc.data buffer and the targets.payloads[] array, but did not validate the per-target data buffers those array elements point at. Each struct i3c_ccc_target_payload carries its own data pointer and data_len, and neither was passed through K_SYSCALL_MEMORY() before the payload was handed to z_impl_i3c_do_ccc() and on to the controller driver. The verifier also operated on the caller's live structure rather than a snapshot, so validated fields could be changed by a second user thread between the check and the driver's use — unlike the sibling z_vrfy_i3c_transfer(), which has always copied its message array first. The defect is only present in CONFIG_USERSPACE builds, where drivers/i3c/i3c_handlers.c is compiled. An unprivileged user-mode thread that has been granted access to the I3C controller device object — the ordinary way an application lets a user thread talk to I3C peripherals — can issue a direct CCC whose target payload data pointer names an arbitrary kernel address. Controller drivers dereference that pointer directly (for example drivers/i3c/i3c_mcux.c, drivers/i3c/i3c_cdns.c, drivers/i3c/i3c_stm32.c, drivers/i3c/i3c_npcx.c), using rnw to decide direction. A read CCC therefore causes the kernel-mode driver to write bus-received bytes into an attacker-chosen kernel address for an attacker-chosen length, and a write CCC transmits kernel memory out onto the I3C bus. The result is an out-of-bounds kernel write plus a kernel memory disclosure, i.e. escalation from a user-mode thread to supervisor privilege, defeating the isolation CONFIG_USERSPACE is meant to provide. The fix introduces copy_ccc_and_do(), which snapshots the payload, copies the target array into kernel memory with k_usermode_alloc_from_copy() (bounding num_targets to fewer than 32), validates each per-target buffer with K_SYSCALL_MEMORY() according to rnw, and copies the driver-written num_xfer and err fields back to the caller.	7.8	More Details
CVE-2026-	ZeroClaw versions before 0.8.5 built with plugins-wasm feature contain a path traversal vulnerability in plugin installation that fails to validate the wasm_path manifest field. Attackers can convince users to		More

101885	install crafted plugins that write arbitrary files to paths outside the plugins directory, such as shell startup files, enabling code execution.	7.8	Details
CVE-2026-12171	auto-changelog before 2.6.1 merges configuration from inside the target repository (the .auto-changelog file and the auto-changelog key in package.json) into its options, and honors security-sensitive options from that untrusted source. The handlebarsSetup option is passed to require(), so running auto-changelog over attacker-controlled repository content (for example, in a CI workflow that checks out an untrusted pull request head, or locally on a forked or third-party repository) executes attacker-chosen code with the privileges of the invoking user or CI job, including access to workflow secrets, without the repository dependencies ever being installed. The plugins option similarly loads attacker-controlled modules from the repository. Under the same conditions, appendGitLog/appendGitTag allow git argument injection (e.g. --output= to write arbitrary files), output allows writing attacker-influenced content to arbitrary paths, and template causes an outbound request to an attacker-chosen URL. Version 2.6.1 treats in-repository configuration as untrusted and refuses to run when it sets these options, unless the new --unsafe-config flag is passed.	7.8	More Details
CVE-2026-103106	Pexip Infinity before 38.2, plus 39.0, 39.1, and 40.0, is affected by improper input validation within an internal Pexip Infinity service that allows an attacker with local access to escalate privileges to root. Exploitation requires an attacker to be able to run arbitrary code on a node by either achieving remote code execution via some other vulnerability or having administrative access to the operating system.	7.8	More Details
CVE-2026-53605	Reachy Mini ISO for Wireless contains the necessary files to build a custom Raspberry Pi OS image for the Reachy Mini Wireless robot, using pi-gen. Prior to version 0.2.4, the Reachy Mini Wireless OS image shipped with an overly broad sudoers entry granting the pollen daemon user (uid 1000) passwordless sudo access to /usr/bin/systemctl with no subcommand or argument restriction. This is a local privilege escalation (LPE). Any process running as pollen can obtain full root (uid 0) on the device in three commands, with no additional vulnerability required and no user interaction. This issue has been patched in version 0.2.4.	7.8	More Details
CVE-2026-47601	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the open-source kernel module DMA-BUF import path where an unprivileged local user could cause improper preservation of memory access permissions when importing a read-only buffer from another device's DMA-BUF exporter. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47489	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where permissions on read-only memory might not be preserved. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47491	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user can cause improper release of memory resources, leaving a mapping accessible after the underlying memory is reused. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47493	NVIDIA vGPU software for Windows and Linux contains a vulnerability in the GPU kernel driver where a guest may access privileged host GPU resources for which it is not authorized. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47494	NVIDIA GPU Display Driver for Linux contains a vulnerability where a user might be able to cause a format string issue. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47495	NVIDIA vGPU Virtual GPU Manager for Windows and Linux contains a vulnerability in the kernel mode layer where a user could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47497	NVIDIA Virtual GPU Manager contains a vulnerability in the GPU System Processor (GSP) tracing component where a guest VM user may cause improper access by sending crafted data through a shared buffer. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47511	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer,		

CVE-2026-47513	where a user could cause an out-of-bounds read from kernel heap memory. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47512	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an out-of-bounds read leading to kernel information disclosure. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-55286	In stpropnci_process of stpropnci.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47561	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where the size of an ioctl input buffer is not validated, allowing an unprivileged caller to trigger an out-of-bounds write in kernel memory. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47560	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-58815	In multiple locations, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47559	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could access memory belonging to another user's process. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-58841	In multiple functions of VirtualAudioControllerTest.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47558	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause a double-free of imported memory state. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47556	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause an integer overflow that leads to an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-58854	In multiple locations, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47553	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47552	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user could bypass an authorization check and modify privileged configuration. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-58859	In multiple places, there is a possible denial of service due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47551	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where a user could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer where an unprivileged local user can supply an untrusted pointer that the driver dereferences without validation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of	7.8	More Details

47550	privileges, information disclosure, and data tampering.		
CVE-2026-47541	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-62146	A trust-boundary flaw in CRI-O's sandbox state persistence allows attacker-influenced pod metadata to overwrite CRI-O's own reserved sandbox bookkeeping; once reloaded as trusted after a restart, a later container recreate in that sandbox can expose a host-side runtime-management resource inside the container, enabling container escape.	7.8	More Details
CVE-2026-47563	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a user could cause a NULL pointer dereference. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-55270	In dialInternal in multiple locations, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47577	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where an attacker could cause an incorrect comparison. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-55269	In FilterCapturedPacket of snoop_logger.cc, there is a possible memory safety issue due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47574	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability where an attacker could cause incorrect resource transfer between spheres. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47573	NVIDIA NVAPI for Windows contains a vulnerability where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47572	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a user could cause type confusion. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47571	NVIDIA GPU Display Driver for Windows contains a vulnerability in kernel-mode escape handling where an attacker with local access could bypass an authorization check that is intended to restrict certain operations based on client execution context. A successful exploit of this vulnerability might lead to escalation of privilege, information disclosure, data tampering, denial of service, or code execution.	7.8	More Details
CVE-2026-49933	In handle_le_monitor_device_event of msft.cc, there is a possible control-flow hijack in the privileged bluetooth process due to an uninitialized pointer dereference. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-49885	In rw_t4t_update_file of rw_t4t.cc, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-49880	In multiple functions of nfa_nfcee_act.cc, there is a possible out-of-bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-55266	In qsort of libufdt_sysdeps_vendor.c, there is a possible out-of-bounds write due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-28648	In Settings, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-28647	In updateState of DeviceAdminAppsPreferenceController.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-	In shouldDisableUninstallButton of ApplicationActionButtonsPreferenceController.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of	7.8	More Details

28641	privilege with no additional execution privileges needed. User interaction is not needed for exploitation.		
CVE-2026-28640	In checkCallerIsCertInstallerOrSelfInProfile of CredentialStorageActivity.java, there is a possible permission bypass due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-28625	In multiple locations, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47570	NVIDIA GPU Display Driver for Windows contains a vulnerability in the CUDA driver where an attacker could cause a library to be loaded from an uncontrolled search path. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, data tampering, and denial of service.	7.8	More Details
CVE-2026-47569	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a user could cause a type confusion via a handle recycle race. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47540	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an integer underflow. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47545	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47528	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the firmware where an attacker could cause an access of an uninitialized pointer. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47520	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47588	NVIDIA GPU Display Driver for Linux contains a vulnerability where an unprivileged user could cause a use-after-free condition by issuing a sequence of driver commands. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service and information disclosure.	7.8	More Details
CVE-2026-47589	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where an unprivileged user may cause a use-after-free condition by issuing a sequence of driver commands. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47523	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47590	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where an unprivileged user may cause a use-after-free condition by issuing a sequence of driver commands. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47591	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user could bypass read-only memory protection due to incorrect authorization, enabling write access to memory marked read-only. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47521	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause an out-of-bounds read. A successful exploit of this vulnerability	7.8	More

47592	might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.		Details
CVE-2026-47593	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer where an unprivileged user can cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, and denial of service.	7.8	More Details
CVE-2026-47594	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where an unprivileged user may cause a use-after-free condition by issuing a sequence of driver commands. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, data tampering, and information disclosure.	7.8	More Details
CVE-2026-47585	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where an attacker could cause an integer underflow. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47519	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47595	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user can write to read-only memory because the memory's permissions are not preserved. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47516	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where an unprivileged user could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2026-47597	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the open-source kernel module Resource Server where an unprivileged local user could cause a use-after-free through a missing self-reference guard in the map cleanup path. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47514	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause exposure of kernel stack contents including return addresses and pointers. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47599	NVIDIA GPU Display Driver for Linux contains a vulnerability in the open-source kernel module where an unprivileged local user could cause improper preservation of memory access permissions during DMA mapping. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-49937	In multiple functions of MessageQueueBase.h, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-47600	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an error-handling path could operate on an improperly initialized resource. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47587	NVIDIA GPU Display Driver for Linux contains a vulnerability where an unprivileged user could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47548	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47530	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer where an attacker could cause an incorrect buffer size calculation. A successful exploit of this vulnerability might		More

2026-47578	lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	Details
CVE-2026-47579	The NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode driver through which a user might trigger a use-after-free condition. Successful exploitation of this issue could lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2026-104026	In Sapling SCM prior to v0.2.20260929-102736, control characters were allowed to be embedded in Git subtree URLs. A maliciously constructed repository, if cloned by a target, could trigger code execution on otherwise read-only actions such as <code>sl log/blame/annotate</code> .	7.8	More Details
CVE-2026-47536	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47535	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the firmware where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-47583	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where an attacker could cause type confusion. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2026-101104	The Meari IoT Cloud Platform OpenAPI Service is vulnerable to an authorization flaw that allows authenticated users to manipulate the configurations of devices they do not own. This vulnerability enables attackers to perform unauthorized actions, such as altering device settings or triggering unintended behaviors, without verifying ownership or permissions.	7.7	More Details
CVE-2026-103757	Budibase through 3.41.0 contains a server-side request forgery vulnerability in AI table generation because the <code>uploadUrl</code> function in <code>packages/server/src/utilities/fileUtils.ts</code> uses <code>raw node-fetch</code> instead of <code>fetchWithBlacklist</code> . Authenticated builder users can send a prompt to <code>POST /api/ai/tables</code> that places an internal URL in an attachment column, causing the server to fetch it and return a presigned object-storage URL containing the response, such as cloud metadata credentials.	7.7	More Details
CVE-2026-103246	n8n versions before 2.39.6 and 2.40.0 before 2.40.1 fail to validate credential ownership during inline agent node-tool introspection. Attackers can reference arbitrary credential IDs to decrypt and exfiltrate plaintext secrets to attacker-controlled hosts without ownership verification.	7.7	More Details
CVE-2026-104977	Plane is an open-source project management tool. Prior to 1.4.0, the fix for CVE-2026-27706 and GHSA-jcc6-f9v6-f7jw, an SSRF in work-item link unfurling shipped in v1.2.2, remains incomplete in the v1.3.1 GA release. Any authenticated project member can make the server fetch attacker-selected internal targets, including cloud metadata at 169.254.169.254, and read the response body returned as the link title or favicon. Complete hardening exists on main in PR 9163 but was not included in an earlier released tag. This issue is fixed in 1.4.0.	7.7	More Details
CVE-2026-100268	In JetBrains YouTrack before 2026.2.19197 project administrators could read comments from other projects via notification templates	7.7	More Details
CVE-2026-82044	UTMStack before 11.2.16 contains a server-side request forgery vulnerability that allows authenticated attackers to make the server request arbitrary internal resources by supplying an unvalidated url parameter to the <code>PdfService.downloadPdf()</code> method exposed via <code>GET /api/generate-pdf-report</code> . Attackers can leverage this to force the web-pdf microservice to fetch internal backend endpoints, the OpenSearch cluster, or the cloud instance-metadata service, exposing sensitive internal data rendered into the returned PDF.	7.7	More Details
CVE-2026-100266	In JetBrains Hub before 2026.2.52366 missing authorisation allowed authenticated users to send arbitrary emails from the server's trusted address	7.7	More Details
CVE-2026-12544	A flaw was found in Foreman. The <code>foreman-rake</code> initialization logic in <code>/usr/share/foreman/config/settings.rb</code> contains a vulnerable code pattern where configuration data is processed through two distinct executable layers. This creates a multi-stage execution chain that allows for both Server-Side Template Injection (SSTI) and insecure deserialization. This vulnerability can lead to remote code execution, total infrastructure compromise and supply chain risk.	7.7	More Details
CVE-2026-103252	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain an authorization bypass vulnerability in the credential test endpoint that resolves project-scoped variables without validating caller access. Attackers can specify an arbitrary project ID in the request body to interpolate sensitive variables into credential test requests sent to attacker-controlled hosts for	7.7	More Details

	exfiltration.		
CVE-2026-78861	An issue in Mercusys AC12 V2 allows a local attacker to execute arbitrary code via a hardcoded 512-bit RSA Private Key	7.7	More Details
CVE-2026-103431	colmux in collectl before 4.3.20.2 does not sanitize ANSI/VT100 terminal escape sequences in data received from remote collectl instances before displaying it, allowing a local user on a monitored host to inject escape sequences into the terminal of an operator running colmux, via a crafted process name (argv[0]).	7.7	More Details
CVE-2026-105208	ZITADEL 4.x before 4.17.3 and 3.x through 3.4.15 protects IdP intent tokens with unauthenticated, malleable encryption, allowing authenticated users to tamper with their own token so it is accepted for another user's external login intent. An attacker who predicts a victim's in-flight intent identifier and wins a timing race can call /v2/idp_intents or /v2/sessions to steal the victim's IdP tokens or hijack their session.	7.7	More Details
CVE-2026-103257	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a path traversal vulnerability in the n8n node that fails to validate resource identifiers. Attackers can craft malicious resource IDs to redirect API calls to unintended resources, allowing unauthorized access to workflows, executions, and credential secrets within the API key's scope.	7.7	More Details
CVE-2026-47576	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module through which an attacker might initiate an out-of-bounds read. Successful exploitation of this issue could lead to denial of service and information disclosure.	7.7	More Details
CVE-2026-103109	Pexip Infinity before 38.2, plus 39.0, 39.1 and 40.0, is affected by improper input validation in the media implementation that allows a remote attacker to trigger memory corruption or a software abort resulting in a denial of service. A crafted media stream may result in a controlled abort during processing, and has the potential to achieve memory corruption.	7.7	More Details
CVE-2026-62097	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPTasty Business Directory business-directory-plugin allows Blind SQL Injection.This issue affects Business Directory: from n/a through 6.4.27.	7.6	More Details
CVE-2026-100262	In JetBrains YouTrack before 2026.2.18991 missing authorisation allowed users with read-only project access to overwrite project notification templates	7.6	More Details
CVE-2026-104408	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Groundhogg Groundhogg groundhogg allows Blind SQL Injection.This issue affects Groundhogg: from n/a through 4.8.3.	7.6	More Details
CVE-2026-62059	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ultimate Member Ultimate Member ultimate-member allows Blind SQL Injection.This issue affects Ultimate Member: from n/a through 2.13.1.	7.6	More Details
CVE-2026-103259	n8n versions before 2.39.6 and 2.40.0 before 2.40.1 contain a session token leakage vulnerability in the Dynamic Credentials authorize and revoke endpoints. Attackers with resolver registration capability can capture collaborators' session tokens by setting a fallback resolver to an attacker-controlled endpoint during the account connection flow, enabling unauthorized credential access.	7.6	More Details
CVE-2026-103249	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a stored DOM cross-site scripting vulnerability in Resource Locator parameter dropdown link handling. Workflow authors can inject malicious script URLs that execute arbitrary JavaScript in the editor origin when other users open the node dropdown and click the external-link icon, with the payload persisting across workflow imports and shares.	7.6	More Details
CVE-2026-62060	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in captivateaudio Captivate Sync captivatesync-trade allows Blind SQL Injection.This issue affects Captivate Sync: from n/a through 3.3.2.	7.6	More Details
CVE-2026-55232	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to version 1.0.8.6, Vvweb's SSRF guard resolves a host with an IPv4-only function and never inspects IPv6, so any host that lacks an A record passes a private-range check. Editor oEmbed proxy fetches an attacker-supplied URL server side and reflects a response body, so an authenticated admin-panel user (default role site_admin or higher) can read internal-only services and cloud metadata, including IAM credentials, using an IPv6 literal or a domain that carries only an AAAA record. This issue has been patched in version 1.0.8.6.	7.6	More Details

CVE-2026-94082	Author SQL Injection in Quiz Cat <= 3.1.1 versions.	7.6	More Details
CVE-2026-103111	PCRE2 before 10.49, when there is an attacker-controlled regular expression and certain JIT API usage, allows an out-of-bounds write with arbitrary data.	7.6	More Details
CVE-2026-96827	Administrator SQL Injection in Admin Notices Manager <= 1.6.0 versions.	7.6	More Details
CVE-2026-97303	Missing Authorization vulnerability in Apps Mav Scratch & Win – Giveaways and Contests scratch-win-giveaways-for-website-facebook allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Scratch & Win – Giveaways and Contests: from n/a through 3.0.2.	7.6	More Details
CVE-2026-104973	Plane is an open-source project management tool. Prior to 1.4.0, the fix for CVE-2026-30242 validates webhook IP addresses only when the webhook is created in apps/api/plane/app/serializers/webhook.py. The delivery task in apps/api/plane/bgtasks/webhook_task.py performs a separate DNS resolution when sending the request and does not validate the resolved IP address, allowing DNS rebinding to bypass the SSRF protection. This issue is fixed in 1.4.0.	7.6	More Details
CVE-2026-103958	Server-side request forgery in the tool server and remote agent connection handling in Loom for AWS before 1.7.0 might allow an authenticated remote user to obtain the credentials of the application's own container role and to read responses from arbitrary internal network locations, via a crafted connection address supplied when registering, updating or testing a tool server or remote agent. To remediate this issue, users should upgrade to version 1.7.0 or later.	7.6	More Details
CVE-2026-96346	Author SQL Injection in WP ERP <= 1.17.9 versions.	7.6	More Details
CVE-2026-96345	Administrator SQL Injection in Estatik <= 4.3.5 versions.	7.6	More Details
CVE-2026-97297	Subscriber Broken Access Control in Gratisfaction <= 4.6.3 versions.	7.6	More Details
CVE-2026-97277	Subscriber Broken Access Control in Social Boost <= 3.6.2 versions.	7.6	More Details
CVE-2026-104456	YesWiki before 4.6.7 contains a second-order SQL injection vulnerability in AcIService::updateRequestWithACL, where a stored username is concatenated unescaped into a read-ACL LIKE clause. Attackers can self-register an account name containing a double-quote payload, then load non-admin ACL-filtered listings to read database contents and bypass read ACLs.	7.6	More Details
CVE-2026-96828	Administrator SQL Injection in Category Discount Woocommerce <= 5.18 versions.	7.6	More Details
CVE-2026-62085	Administrator SQL Injection in WP Activity Log <= 5.6.6 versions.	7.6	More Details
CVE-2026-105628	Plane is an open-source project management tool. Prior to 1.4.0, Plane's OAuth avatar synchronization flow fetches avatar_url from provider user data through a server-side HTTP request without internal IP validation and follows redirects by default. An attacker can provide an avatar URL that redirects to an internal-only resource, such as a metadata endpoint, and Plane uploads the fetched response as a user avatar file. The object is then exposed through /api/assets/v2/static/{asset_id}/, allowing exfiltration of internally fetched content. This issue is fixed in 1.4.0.	7.6	More Details
CVE-2026-104460	YesWiki before 4.6.7 contains a blind SQL injection vulnerability in the {{newtextsearch}} action because Bazar list option ids are concatenated into SQL REGEXP/LIKE clauses in actions/newtextsearch.php without escaping. Anonymous attackers can plant a malicious option id in an anonymously editable Bazar list and use search requests as a boolean oracle to read arbitrary database data, including admin password hashes from the yeswiki_users table.	7.5	More Details

CVE-2026-56661	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. Prior to version 1.5, the update handler fetches a user-supplied URL with <code>file_get_contents()</code> after only format validation (<code>FILTER_VALIDATE_URL</code>) — there is no validation of the request destination. An attacker who can submit the form can make the server issue requests to arbitrary destinations, including internal-only services and cloud metadata endpoints (169.254.169.254). The fetched response body is written to a web-accessible file (<code>/Tmpfile.zip</code>) and is not deleted when the content is not a valid ZIP, turning this into a full-read SSRF: the attacker can retrieve the response of the internal request directly. This issue has been patched in version 1.5.	7.5	More Details
CVE-2026-103097	An API key is hardcoded and retrievable from the application package. Since Android applications can be reverse engineered, embedding sensitive API credentials directly in the client application may allow unauthorized users to extract and misuse the key.	7.5	More Details
CVE-2026-58865	In multiple functions of <code>PduParser.java</code> , there is a possible persistent denial of service due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2026-85532	Apache WSS4J accepted attacker-controlled derived-key lengths and offsets without adequate bounds. This could permit cryptographically weak keys or excessive CPU and memory consumption when processing crafted WS-Security messages. The fixes enforce a minimum key length of 16 bytes, a maximum length of 512 bytes, and a maximum offset of 4096 bytes. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4, which fix this issue.	7.5	More Details
CVE-2026-89294	The Simply Schedule Appointments plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.6.12.27 via the <code>'ssa_locale'</code> parameter parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to include and execute arbitrary <code>.php</code> files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where <code>.php</code> file types can be uploaded and included. Notably, exploitation does not require authentication in practice, as the locale filter is installed unconditionally on every request during <code>plugins_loaded</code> and the callback performs no nonce or capability check before returning the raw GET parameter value.	7.5	More Details
CVE-2026-103098	Transmission of a sensitive key in the URL over an unencrypted HTTP connection. The request is sent over HTTP rather than HTTPS, meaning the key is transmitted in plaintext across the network. An attacker with the ability to monitor network traffic could intercept the request and obtain the key	7.5	More Details
CVE-2026-104416	Ghost from 4.39.0 before 6.64.0 contains an information disclosure vulnerability in the Admin API that allows staff users to view secret tokens of pending staff invites. Staff users with invite viewing permission can accept pending invites for higher-privileged roles to escalate their privileges.	7.5	More Details
CVE-2026-104410	SiYuan before 3.8.5 contains an information disclosure vulnerability that allows publish readers to read password-protected and publish-disabled database rows via the <code>/api/export/preview</code> endpoint. Attackers can request an export preview of a public document embedding a database view to obtain protected rows' primary-key text and cell values.	7.5	More Details
CVE-2026-89193	The Robin Image Optimizer WordPress plugin before 2.0.8 does not escape values that its bundled HTML parser re-emits into element attributes when a non-default image delivery mode is enabled, allowing unauthenticated users to submit content that is stored and later executed as Cross-Site Scripting in the browser of any user viewing an affected page, including administrators.	7.5	More Details
CVE-2026-97337	The Simple Membership plugin for WordPress is vulnerable to unauthorized modification of data and sensitive information disclosure in versions up to, and including, 4.8.3 via the <code>resend-activation</code> and <code>email-activation</code> endpoints. The endpoints are dispatched from <code>SwpmInitTimeTasks::check_and_do_email_activation()</code> on frontend init with no authentication, nonce, capability, or ownership check, and the recipient address used by <code>SwpmRegistration::send_reg_email()</code> is taken from an attacker-controlled <code>\$_POST['email']</code> parameter (overriding the member's registered address). This makes it possible for unauthenticated attackers to redirect an arbitrary pending member's activation email — and the follow-up 'registration complete' email containing the member's username and plaintext password — to an attacker-chosen address, and to then activate that member's account without their consent.	7.5	More Details
CVE-2026-91828	The OMGF GDPR/DSGVO Compliant, Faster Google Fonts. Easy. WordPress plugin before 6.3.11 does not require authentication or a valid nonce on an action that issues a slow server-side loopback request, allowing unauthenticated attackers to exhaust the site's PHP worker pool and make the entire site unavailable.	7.5	More Details
	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.73.2 via the <code>'theme'</code> parameter parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary <code>.php</code>		

CVE-2026-92174	files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. Exploitation requires sending a malicious widgetData payload containing a legacy top-level theme key alongside a non-empty columns array to the /wp-json/sowb/v1/widgets/previews REST endpoint, which bypasses field validation because update_fields() only processes declared form fields.	7.5	More Details
CVE-2026-96267	The WP Visitor Statistics (Real Time Traffic) plugin for WordPress is vulnerable to generic SQL Injection via the 'fullRef' parameter in all versions up to, and including, 8.7 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. This is a second-order SQL injection: an unauthenticated attacker submits a crafted referrer URL to the wmcTrack tracking endpoint, which persists the raw unescaped value into the wp_logVisit table, and the injection is triggered when an administrator next views the Traffic Sources dashboard.	7.5	More Details
CVE-2026-93882	The LearnPress – WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 4.4.8 via the CourseMaterialTemplate::render_material_items() callback exposed on the public lp-ajax-handle (load_content_via_ajax) endpoint. The endpoint is explicitly listed in the AbstractAjax no-nonce allowlist and performs no capability check, and the render_material_items() handler decides authorization against one attacker-supplied identifier (course_id) while fetching the returned material rows via a second, independently attacker-supplied identifier (item_id) with no check that the lesson belongs to the authorized course. This makes it possible for unauthenticated attackers to read and download course-material files (uploaded and external file paths/URLs) belonging to lessons in paid or enrollment-required courses, provided any single course on the site has 'No Required Enroll' enabled and owns at least one material file.	7.5	More Details
CVE-2026-96255	The Payments for Hubtel WordPress plugin before 1.0.2 does not prevent public access to a debug log in which it records payment requests, including the store's payment gateway API credentials in plain text, allowing unauthenticated attackers to obtain those credentials.	7.5	More Details
CVE-2026-104472	YesWiki before 4.6.7 contains a missing authorization vulnerability in the attachment download handler that allows unauthenticated attackers to bypass page read ACLs. Attackers can request the download handler with a known page tag and file parameter to retrieve confidential attachments from read-restricted pages.	7.5	More Details
CVE-2026-103096	API key is hardcoded and retrievable from the application package. Since Android applications can be reverse engineered, embedding sensitive API credentials directly in the client application may allow unauthorized users to extract and misuse the key.	7.5	More Details
CVE-2026-103761	Mooncake transfer engine through 0.3.13.post1 contains a memory exhaustion vulnerability in TransferMetadata::receivePeerNotify that allows unauthenticated attackers to grow process memory without limit. Attackers can repeatedly send notify frames up to 1 MB to the handshake RPC port, filling the uncapped notifiys vector until the out-of-memory killer terminates the engine.	7.5	More Details
CVE-2026-104020	Uncontrolled recursion in the lon reader in Amazon lon Python before 0.15.0 might allow a remote unauthenticated actor to crash the application using the library, resulting in a denial of service, via a crafted, deeply nested lon value. To remediate this issue, users should upgrade to version 0.15.0 or later.	7.5	More Details
CVE-2026-94002	Possible memory exhaustion in SFTP clients (DefaultSftpClient) in component sshd-sftp in Apache MINA SSHD versions 0.9.0 to 2.19.0 and 3.0.0-M1 to 3.0.0-M5. Apache MINA SSHD is a Java library for client-side and server-side SSH. The sshd-sftp component provides support for SFTP. The SFTP client implementation, when receiving a reply, did not check that this reply corresponded to a request sent earlier. Unsolicited replies would be stored but never consumed. A malicious server could keep sending unsolicited replies until available memory in the client was exhausted. Users are recommended to upgrade to version 2.20.0 or 3.0.0-M6, which fix this issue.	7.5	More Details
CVE-2026-104462	YesWiki before 4.6.7 contains an SQL injection vulnerability in the Bazar nuagetag action, which concatenates the unescaped tags attribute into a raw SQL IN clause. Attackers with page-write access (unauthenticated on default installs) can embed a nuagetag tag ending in a backslash to break quote parity and inject a UNION subquery, exfiltrating password hashes and arbitrary table data.	7.5	More Details
CVE-2026-75098	The Product Designer App plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.1.3 via the 'svg' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. The endpoint's only authentication gate relies on a nonce and token that are both publicly emitted as JavaScript globals on any page rendering the [pdapp-studio-page] shortcode, making them freely	7.5	More Details

	obtainable by anonymous visitors.		
CVE-2026-51874	In Devika v1.0, the Patcher Agent save_code_to_project function contains a path traversal vulnerability that allows attackers to write files outside the intended project workspace.	7.5	More Details
CVE-2026-51888	langflow-ai langflow v1.8.4 is affected by: Directory Traversal. The impact is: Arbitrary file write outside the intended workspace or storage boundary.. The component is: src/backend/base/langflow/api/v1/knowledge_bases.py:knowledge_bases-create_knowledge_base-a-live-http-post-to-create-knowledge-base. The attack vector is: Attack surface: HTTP or browser-backed service path. A public-facing upload or HTTP route handler forwards an attacker-controlled path or filename into host file creation without any visible boundary enforcement. ¶¶ A weakness has been identified in langflow-ai langflow up to 1.8.4. langflow contains an absolute path traversal vulnerability in knowledge_bases-create_knowledge_base-a-live-http-post-to-create-knowledge-base (src/backend/base/langflow/api/v1/knowledge_bases.py:51). An attacker can write or overwrite files outside the intended working directory by providing absolute paths in the knowledge base creation endpoint.	7.5	More Details
CVE-2026-104431	Zebra before 6.0.0 contains a denial of service vulnerability that allows unauthenticated peers to stall Tokio workers by submitting mempool transactions requiring expensive synchronous script verification. Attackers can send non-standard high-sigop P2SH transactions that reach CachedFfiTransaction::is_valid() before standardness checks, saturating the verifier buffer and rendering the node unresponsive.	7.5	More Details
CVE-2026-104430	Zebra zebra4.5.0 and zebra-script 7.0.0 count P2SH redeem script signature operations in legacy mode rather than zcashd's accurate P2SH mode, overcounting CHECKMULTISIG preceded by OP_1 through OP_16 as 20 sigops and causing a consensus divergence. Remote attackers can broadcast P2SH spends using low-threshold multisig redeem scripts so that a block zcashd accepts exceeds Zebra's inflated MAX_BLOCK_SIGOPS count, causing Zebra nodes to reject it and stall off the chain.	7.5	More Details
CVE-2026-102999	pypdf is a free and open-source pure-python PDF library. Prior to 6.19.0, a crafted PDF containing many embedded files can cause the dictionary-based attachments API in pypdf/_doc_common.py to reparse the full attachment list for each content lookup, producing repeated work and long runtimes when an application accesses the embedded-file mapping. This issue is fixed in version 6.19.0.	7.5	More Details
CVE-2026-6806	The Motors - Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'stm_lat/stm_lng' parameter in all versions up to, and including, 1.4.109 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-2026-104712	Asymmetric resource consumption (amplification) vulnerability in Apache Struts. When a request parameter is bound to an arbitrary-precision decimal (java.math.BigDecimal) property that is then rendered through the Struts tag library, the framework can produce a response many orders of magnitude larger than the request, allowing an unauthenticated remote attacker to exhaust server CPU and outbound network capacity with sustained low-volume traffic. Applications that do not bind request parameters to BigDecimal properties, or never render such a property through the Struts tag library, are not affected. This issue affects Apache Struts: from 2.5.14 through 2.5.33, from 6.0.0 through 6.11.0, from 7.0.0 through 7.3.0. Users are recommended to upgrade to version 6.12.0 or 7.4.0, which fixes the issue.	7.5	More Details
CVE-2026-86134	A NULL pointer dereference vulnerability in the WatchGuard Fireware OS authentication process allows a remote, unauthenticated attacker to crash the management daemon by sending a specially request to the login interface, resulting in a denial of service.	7.5	More Details
CVE-2026-86344	A flaw was found in 389-ds-base. An unauthenticated remote attacker can send a complete LDAP operation followed by the first bytes of an incomplete LDAPMessage on the same connection, causing the server to hand that connection to a second worker thread before the first worker's result is flushed. The second worker blocks until nsslapd-ioblocktimeout while holding the connection mutex, preventing delivery of the completed operation's result. Repeating this across a small number of connections proportional to the configured worker-thread pool size exhausts the entire pool under default configuration, denying service to all clients (anonymous and authenticated, plaintext and TLS) for as long as the attacker maintains the connections.	7.5	More Details
CVE-2026-76992	The CODESYS Gateway Client allocates memory based on a size field in a gateway response without enforcing an appropriate upper limit. An unauthenticated remote attacker controlling a malicious gateway can exploit this behavior to trigger excessive memory consumption, resulting in a denial-of-service condition thus leading to a total loss of availability.	7.5	More Details

CVE-2026-75028	The WPCafe – Restaurant Menu, Online Food Ordering & Table Booking System plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.0.18 via the (template scope) function. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	7.5	More Details
CVE-2026-103334	Insertion of Sensitive Information Into Sent Data vulnerability in Etoile Web Design Incorporated Five Star Restaurant Reservations restaurant-reservations allows Retrieve Embedded Sensitive Data.This issue affects Five Star Restaurant Reservations: from n/a through 2.7.24.	7.5	More Details
CVE-2026-104422	The block sync download path in Zebra (zebrad) before 6.3.0 reads a block's height from its unvalidated coinbase scriptSig and drops blocks that appear too far behind the tip before consensus validation, without penalizing the supplying peer. Because V5 transaction IDs exclude the scriptSig, a malicious peer can repeatedly serve a canonical block whose coinbase claims height 1 while keeping the requested hash, delaying the node's discovery of the newest block.	7.5	More Details
CVE-2026-104891	mppx-condition-gate provides conditional free-access wrappers for mppx payment methods. Prior to @insumermodel/mppx-condition-gate 3.0.0 and @insumermodel/mppx-token-gate 1.0.4, the packages read a wallet address from the client-supplied credential.source, checked whether that public address met configured on-chain conditions, and returned a successful free-access receipt without invoking the wrapped payment verifier or proving that the caller controlled the wallet. An unauthenticated attacker could name any qualifying wallet and obtain content that should require payment, and cached grants could be reused for the configured cache lifetime. The corrected packages prevent free-access authorization unless payer control has been established. These issues are fixed in @insumermodel/mppx-condition-gate 3.0.0 and @insumermodel/mppx-token-gate 1.0.4.	7.5	More Details
CVE-2026-105675	Ghost is a Node.js content management system. From 4.39.0 until 6.64.0, staff users with permission to view staff invites were able to discover the secret token of pending invites, including invites for roles with higher privileges than their own. This could allow a staff user to escalate their privileges by accepting a pending invite. This issue is fixed in version 6.64.0.	7.5	More Details
CVE-2026-86104	An uncontrolled resource consumption vulnerability in the Fireware OS login process (wgagent) allows a remote, unauthenticated attacker to cause a denial of service by sending a specially crafted request.	7.5	More Details
CVE-2026-102091	Kiteworks Secure Data Forms before version 9.5.0 is vulnerable to Server-Side Request Forgery that could allow an unauthenticated, remote attacker to make the server issue arbitrary outbound network requests and read back the responses. This could potentially be used to reach internal-only services or other network-restricted resources.	7.5	More Details
CVE-2026-92245	The Simply Schedule Appointments plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.6.12.32 via the 'recursive' parameter. This makes it possible for unauthenticated attackers to extract customer PII — including names, email addresses, phone numbers, and custom form field data — stored in appointment records, as well as per-appointment public_token values. The leaked per-appointment public_token values also enable unauthenticated attackers to delete arbitrary appointments via the DELETE /wp-json/ssa/v1/appointments/{id} endpoint, which accepts the token as sole authorization.	7.5	More Details
CVE-2026-97307	Insertion of Sensitive Information Into Sent Data vulnerability in StylemixThemes Cost Calculator Builder cost-calculator-builder allows Retrieve Embedded Sensitive Data.This issue affects Cost Calculator Builder: from n/a through 4.0.17.	7.5	More Details
CVE-2026-103055	AiSOC versions 7.5.0 before 12.0.0 use a hard-coded constant for JWT verification in the realtime WebSocket and SSE service when the AISOC_REALTIME_JWT_SECRET environment variable is not set. Unauthenticated attackers can forge subscription tickets with arbitrary tenant identifiers to access cross-tenant live alerts, cases, agent events and graph updates through the realtime endpoints.	7.5	More Details
CVE-2026-105212	ZITADEL 3.x before 3.4.14 and 4.x before 4.16.2 contains an authentication bypass in the hosted Login V1 and Login V2 UIs that accepts passkey or other authenticator enrollment on identify-only login sessions, before any primary factor is verified. Unauthenticated attackers knowing only a victim's login name can register an attacker-controlled authenticator and log in as that user, bypassing existing passwords and MFA.	7.5	More Details
CVE-2026-86133	An integer underflow vulnerability in the WatchGuard Fireware OS IKE daemon (iked) allows a remote attacker who has completed the initial IKEv2 handshake to crash the iked process by sending a specially crafted encrypted IKEv2 message, resulting in a denial of service.	7.5	More Details

CVE-2026-86132	An integer underflow vulnerability in the WatchGuard Firewall OS IKEv2 daemon (iked) allows a remote, unauthenticated attacker to crash the process by sending a specially crafted encrypted IKEv2 message negotiated with an AES-GCM cipher suite.	7.5	More Details
CVE-2026-86128	A NULL pointer dereference vulnerability in Fireware OS's NetFlow packet-processing feature allows a remote, unauthenticated attacker to cause a denial of service by sending a specially crafted IPv6 packet.	7.5	More Details
CVE-2026-103591	DeepWiki-Open through commit d92819a contains an unauthenticated arbitrary file read vulnerability in the GET /codemap/file endpoint via the repo_url parameter. Attackers can supply a non-URL repo_url value to bypass path containment checks and read any file accessible to the API process by specifying absolute file paths.	7.5	More Details
CVE-2026-102128	An identity-verification weakness in Kiteworks Email Protection Gateway allowed the gateway to act on the Kiteworks platform on behalf of a user it had not authenticated, and to provision a platform account for an identity it did not already know. A remote, unauthenticated sender could potentially exploit this to obtain control of a platform account.	7.5	More Details
CVE-2024-58387	Inspur Haiyue HCM Cloud contains an arbitrary file read vulnerability in the /api/model_report/file/download endpoint that allows unauthenticated remote attackers to read arbitrary files by supplying unvalidated path parameters index and ext. Attackers can craft requests such as /api/model_report/file/download?index=/ <u>&ext=<path></u> to traverse the filesystem and disclose sensitive files including /etc/passwd, application database files, and system configuration files. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-11-04 .	7.5	More Details
CVE-2026-105219	Mammoth.js 1.3.0 before 1.12.3 contains a regular expression denial of service vulnerability in the style map tokeniser in lib/styles/parser/tokeniser.js due to overlapping regex alternatives. Attackers can supply a crafted .docx with an unterminated quoted string of repeated backslash escapes in mammoth/style-map to block the Node.js event loop.	7.5	More Details
CVE-2026-95265	Feehi CMS 2.1.1 contains a Server-Side Request Forgery (SSRF) vulnerability in the UEditor catchimage endpoint. The private-IP validation does not block loopback or link-local addresses, allowing an attacker to make the server probe internal HTTP services through response differences.	7.5	More Details
CVE-2026-51860	bisheng 2.3.0, 2.4.0, and 2.4.0-beta1 is vulnerable to Directory Traversal in src/backend/bisheng/linsight/domain/task_exec.py.	7.5	More Details
CVE-2026-51853	agent-zero 1.7, 1.8, 1.9, and 1.10 is vulnerable to Directory Traversal in python/helpers/file_browser.py:FileBrowser.__init__. The FileBrowser class initializes with the host root directory as the workspace, allowing the agent to access any file on the system without restriction.	7.5	More Details
CVE-2026-102143	An unauthenticated attacker could cause a file with attacker-controlled content to be written to the appliance filesystem through an administrative upload handler that did not properly authenticate the request. This did not by itself result in code execution, which would require a separate vulnerability to place the file in an executable location.	7.5	More Details
CVE-2026-103000	pypdf is a free and open-source pure-python PDF library. Prior to 6.19.0, a crafted PDF can provide unusually large alphabetical page-label values that cause pypdf/_page_labels.py to generate strings beyond a reasonable page-label length when an application retrieves document page labels, consuming excessive memory and potentially making the application unavailable. This issue is fixed in version 6.19.0.	7.5	More Details
CVE-2026-102995	pypdf is a free and open-source pure-python PDF library. Prior to 6.18.1, a crafted PDF can place unusually large source-code or destination-string tokens in a font /ToUnicode mapping, causing pypdf/_cmap.py parse_bfchar to decode and retain oversized values during operations such as text extraction and consume excessive memory. This is a second follow-up to earlier /ToUnicode resource-consumption fixes and is limited to the remaining token-length path. This issue is fixed in version 6.18.1.	7.5	More Details
CVE-2026-102996	pypdf is a free and open-source pure-python PDF library. Prior to 6.18.1, a crafted PDF can provide a TrueType or Type1 simple font with an unusually large /Widths array, causing pypdf/_font.py Font_collect_tt_t1_character_widths to process entries beyond the 256 character codes meaningful for a simple font and consume excessive memory during operations such as text extraction. This issue is fixed in version 6.18.1.	7.5	More Details
CVE-2026-	pypdf is a free and open-source pure-python PDF library. Prior to 6.18.1, a crafted PDF containing a partially malformed /FlateDecode stream with padded data can force pypdf/filters.py to use inefficient byte-by-byte decompression while the earlier recovery counter fails to advance for bytes that	7.5	More Details

102997	successfully decode, causing long runtimes and application unavailability. This is a residual issue after the malformed FlateDecode recovery fix. This issue is fixed in version 6.18.1.		
CVE-2026-105295	GitAhead 2.5.0 through 2.7.1 contains an insecure update mechanism that installs downloaded updates without integrity or signature verification and permanently ignores TLS errors after one SSL error dialog. Network attackers presenting an invalid certificate once can intercept later automatic update checks, offer a fake version, and execute code as the user upon installation.	7.5	More Details
CVE-2023-54403	Yonyou U8 CRM before V16.5 and V18 contains an arbitrary file read vulnerability in /ajax/getemaildata.php that allows unauthenticated attackers to bypass authentication using the DontCheckLogin=1 parameter and read arbitrary files via an unvalidated filePath parameter. Attackers can exploit this flaw to read sensitive files outside the web application directory, including configuration files containing database or service credentials. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-14.	7.5	More Details
CVE-2026-105631	Plane is an open-source project management tool. Prior to 1.4.0, WorkspaceFileAssetEndpoint.get and WorkspaceAssetDownloadEndpoint.get resolve FileAsset records within a workspace without checking membership in the asset's project, allowing a workspace member to download assets from private projects when the asset UUID is known. EntityAssetEndpoint.get is a separate public-anchor endpoint that grants AllowAny access and scopes the lookup only to the anchor's workspace rather than its published entity or project. An unauthenticated caller who knows a valid anchor and an asset UUID can therefore retrieve issue-description or comment-description assets belonging to unpublished or private projects in that workspace. This issue is fixed in 1.4.0.	7.5	More Details
CVE-2026-103880	Asymmetric Resource Consumption vulnerability in Apache Directory LDAP API. Storing a password using the bcrypt algorithm with a high force like 30 in a LDAP server that supports this algorithm will cause the server CPU to run for hours checking the credentials. A bounded cost should be enforced to avoid a server DOS. This issue affects Apache Directory LDAP API: from 2.1.0 before 2.1.9. Users are recommended to upgrade to version 2.1.9, which fixes the issue.	7.5	More Details
CVE-2026-103472	restbed through 5.0.0 accepts WebSocket frames with declared payload lengths up to 2^63 bytes and buffers the payload without size limits in an unbounded stream buffer. Remote unauthenticated attackers can declare large frame sizes and stream payload data to exhaust server memory, causing denial of service through process crash.	7.5	More Details
CVE-2026-81809	The Paytm Payment Gateway WordPress plugin before 2.8.9 does not properly escape data taken from payment callbacks before using it in a SQL statement, and the integrity check on those callbacks can be forged when the gateway is enabled without credentials, allowing unauthenticated users to perform SQL injection attacks.	7.5	More Details
CVE-2026-81739	The Paytm Payment Gateway WordPress plugin before 2.8.9 does not sanitize and escape data it stores from payment callbacks before outputting it in an admin page, and the integrity check on those callbacks can be forged when the gateway is enabled without credentials, allowing unauthenticated users to store scripts that will run in the session of a store administrator.	7.5	More Details
CVE-2026-103108	Pexip Infinity before 38.2, plus 39.0, 39.1, and 40.0, is affected by improper input validation in the media implementation that allows a remote attacker to trigger a software abort resulting in a denial of service	7.5	More Details
CVE-2026-20526	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: MOLY01898195; Issue ID: MSV-8906.	7.5	More Details
CVE-2026-103104	Pexip Infinity before 38.2, plus 39.0, 39.1 and 40.0, is affected by improper input validation in the media implementation which allows a remote attacker to trigger a software abort resulting in a denial of service.	7.5	More Details
CVE-2026-103100	Pexip Infinity before 40.1 is affected by improper input validation in the signaling implementation that allows a malicious attacker to trigger a software abort resulting in a denial of service.	7.5	More Details
CVE-2026-80276	Comelit Multi-User Gateway for VIP System (model 1456B) firmware versions 2.9.1 and 2.10.0 expose a network-accessible management interface that does not require authentication. Through this interface, sensitive device configuration data - including the Remote Configuration Password - can be read in cleartext by a remote, unauthenticated attacker.	7.5	More Details
CVE-2026-103099	Pexip Infinity before 41.1 is affected by improper input validation in the media implementation that allows a remote attacker to trigger a software abort resulting in a denial of service.	7.5	More Details

CVE-2026-103878	Cleartext transmission of sensitive information vulnerability in Apache Directory LDAP API. A StartTLS extended operation started after a Search request has been sent can lead to receive data in plain text before the TLS Handshake has been completed. This issue affects Apache Directory LDAP API: from 2.1.0 before 2.1.9. Users are recommended to upgrade to version 2.1.9, which fixes the issue.	7.5	More Details
CVE-2023-54402	iDocView contains a server-side request forgery vulnerability in its /doc/upload endpoint that allows remote unauthenticated attackers to fetch arbitrary URLs by supplying a hardcoded default token value (testtoken) to bypass authentication. Attackers can exploit the unrestricted URL scheme handling, including file:// URIs, to read arbitrary local files such as operating-system and application configuration files, and to reach internal network hosts and services not otherwise accessible. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-03-26.	7.5	More Details
CVE-2026-82826	Hitachi Coding Software Suite contains a vulnerability related to the Cleartext Transmission of Sensitive Information which allows an attacker to eavesdrop on with authentication credentials and sensitive data in transit. This issue affects Hitachi Coding Software Suite: through 3.3.0.	7.5	More Details
CVE-2026-88779	Vulnerability in NetScaler ADC and NetScaler Gateway. This issue affects ADC: before 14.1-73.41, before 13.1-64.28, before 14.1-73.41 FIPS, and before 13.1-37.282; Gateway: before 14.1-73.41 and before 13.1-64.28.	7.5	More Details
CVE-2026-101884	OpenClaw Windows Node before 2026.7.1 contains an incomplete environment-variable sanitizer in system.run that fails to block GIT_CONFIG_*, DOTNET_STARTUP_HOOKS, and JAVA_TOOL_OPTIONS variables. Attackers with gateway or agent access can supply these variables to allowlisted tools like git, dotnet, or java to load attacker-controlled code and achieve arbitrary code execution.	7.5	More Details
CVE-2026-103088	Handlebars.java before 4.5.5 allows directory traversal. In handlebars-springmvc 4.5.3 and 4.5.4, the path-containment fix for CVE-2026-63490 validates template locations as raw percent-encoded strings, whereas the template file is opened through a URL handler that percent-decodes the path. In a Spring MVC application with a file: template prefix and a request-derived view name, a percent-encoded traversal such as %2e%2e/ bypasses both the view-resolver check and the loader-side containment and reads files outside the configured template base directory.	7.5	More Details
CVE-2026-102731	Memory allocation with excessive size value vulnerability in Apache Directory LDAP API. A malicious peer (or a MITM) can send a small BER-encoded response causing a large memory allocation before any data is received. This can lead to an OutOfMemoryError and denial of service. The client JVM OOMs (OutOfMemoryError bypasses the DecoderException handlers) or pins the large allocation per connection while the attacker stalls. A handful of connections exhausts any heap. The same bytes from an unauthenticated pre-bind client hit any embedding server that did not set MAX_PDU_SIZE_ATTR. This issue affects Apache Directory LDAP API: from 1.2.0 before 1.2.9. Users are recommended to upgrade to version 1.2.9, which fixes the issue.	7.5	More Details
CVE-2026-102993	pypdf is a free and open-source pure-python PDF library. Prior to 6.17.0, a crafted PDF can provide unusually large Roman page-label values that cause pypdf/_page_labels.py to generate excessively large numeral strings when an application retrieves document page labels, consuming large amounts of memory and potentially making the application unavailable. This issue is fixed in version 6.17.0.	7.5	More Details
CVE-2026-102994	pypdf is a free and open-source pure-python PDF library. Prior to 6.18.0, a crafted PDF containing indirect-object identifiers or generation-number tokens that continue for a long time without whitespace can cause pypdf/_reader.py and pypdf/generic/_base.py to scan excessive input through read_until_whitespace, resulting in long runtimes and application unavailability. This issue is fixed in version 6.18.0.	7.5	More Details
CVE-2026-20520	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01778988; Issue ID: MSV-8897.	7.5	More Details
CVE-2026-20519	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01778993; Issue ID: MSV-8898.	7.5	More Details
CVE-2026-103471	restbed through 5.0.0 buffers HTTP request headers without enforcing a maximum size limit, allowing remote unauthenticated attackers to exhaust server memory. Attackers can open TCP connections and stream bytes indefinitely without sending the header delimiter, forcing the server to allocate unbounded heap memory until the process is killed.	7.5	More Details
CVE-	Zebra (zebrad) before 6.2.1 contains an asymmetric resource consumption vulnerability that allows unauthenticated peers to stall block verification by pushing V6 mempool transactions with invalid Halo2		More

2026-104423	proofs. Attackers can flood the shared unprioritized Halo2 verification queue with zero-fee transactions carrying zero-filled Orchard and Ironwood proofs, causing nodes to fall behind the chain tip.	7.5	Details
CVE-2026-102998	pypdf is a free and open-source pure-python PDF library. Prior to 6.19.0, a crafted PDF with form field values can cause pypdf/generic/_appearance_stream.py appearance-stream generation to repeat invariant selection-data work inside a loop when an application updates fields with flattening enabled, resulting in excessive runtimes and application unavailability. This issue is fixed in version 6.19.0.	7.5	More Details
CVE-2026-62073	Unauthenticated Broken Access Control in WP Full Stripe Free <= 8.5.6 versions.	7.5	More Details
CVE-2026-103272	Ghost versions from 2.10.0 before 6.63.0 contain a staff enumeration vulnerability in the content API that allows unauthenticated attackers to leak user data. Attackers can observe discrepancies in API metadata responses to enumerate staff members and extract sensitive information without authentication.	7.5	More Details
CVE-2026-48005	Missing authentication checks in mod_auth_digest in Apache Software Foundation Apache HTTP Server before 2.4.69 on all platforms allows an unauthenticated remote client to cause a denial of service (forced re-authentication) via forged Authorization headers when Digest authentication is enabled with AuthDigestNcCheck . Users are recommended to upgrade to version 2.4.69, which fixes this issue.	7.5	More Details
CVE-2026-97197	Unauthenticated Broken Access Control in WordPress Backup & Migration <= 1.6.0 versions.	7.5	More Details
CVE-2026-96818	Unauthenticated Broken Access Control in WP Express Checkout (Accept PayPal Payments) <= 2.4.9 versions.	7.5	More Details
CVE-2026-47360	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache HTTP Server's mod_session_cookie module. When SessionCookieRemove changes across internal redirects, the session cookie may still be passed to a backend server. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	7.5	More Details
CVE-2026-94178	Subscriber Privilege Escalation in Import and export users and customers <= 2.5.2 versions.	7.5	More Details
CVE-2026-51916	TransformerOptimus SuperAGI v0.0.14 contains an incorrect access control vulnerability in delete_user_knowledge in superagi/controllers/knowledges.py. In affected source snapshots, POST /knowledges/delete/{knowledge_id} deletes the selected knowledge object without requiring authentication in the route and without verifying organization ownership of the supplied knowledge_id.	7.5	More Details
CVE-2026-46729	NULL Pointer Dereference vulnerability in Apache HTTP Servers mod_heartmonitor over unicast listener. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	7.5	More Details
CVE-2026-97240	Unauthenticated Sensitive Data Exposure in StifLi Backup Tools <= 2.2.7 versions.	7.5	More Details
CVE-2026-100517	Unauthenticated Insecure Direct Object References (IDOR) in Photo Reviews for WooCommerce <= 1.2.30 versions.	7.5	More Details
CVE-2026-95587	Unauthenticated Broken Access Control in Hostinger Migrator <= 1.0 versions.	7.5	More Details
CVE-2026-95616	An integer overflow in WSS4J's DER bounds check lets an oversized allocation pass validation. An unauthenticated attacker can send a SOAP message carrying an X.509 certificate whose SubjectKeyIdentifier extension declares a length of 0x7FFFFFFF; WSS4J decodes this while resolving the signature's key reference, before the message is authenticated, so an eleven-byte extension triggers a 2 GB allocation. Repeated requests exhaust server memory. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4, which fix this issue.	7.5	More Details
CVE-2026-	Unauthenticated Sensitive Data Exposure in BackupEase <= 2.2.2 versions.	7.5	More Details

97241			
CVE-2026-105314	Papermerge 3.5.3 allows remote code execution by a standard user via directory traversal in a /api/documents/upload call. A Python .pth file can be written to site-packages, and its code is executed upon the next start of the Python interpreter.	7.5	More Details
CVE-2026-67989	crmne/ruby_llm at commit fa6f279847d6d7027814539d9c0dfc3bbdfd2a83 contains a polynomial-time regular expression denial-of-service condition in Mistral model capability matching on Ruby 3.1.x	7.5	More Details
CVE-2026-63718	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') response smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi and a crafted uwsgi response with Transfer-Encoding. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.68.	7.5	More Details
CVE-2026-12423	A flaw was found in Foreman. The Red Hat Satellite /unattended/provision API endpoint is vulnerable to an authentication bypass due to a semantic logic flaw in host_verifier.rb. The application verifies the database state of a provisioning token rather than its actual presence in the incoming HTTP request. Because a host actively undergoing provisioning has an unexpired token in the database, the server's valid_host_token? method evaluates to true, granting access to the kickstart template even if the requester provides no token at all in the URL.	7.5	More Details
CVE-2026-63686	A NULL pointer dereference in mod_xml2enc in Apache Software Foundation Apache HTTP Server before 2.4.69 on all platforms allows an untrusted backend server to cause a denial of service via a proxied response with a charset whose conversion partially succeeds then fails. Users are recommended to upgrade to version 2.4.69, which fixes this issue.	7.5	More Details
CVE-2026-47097	AJA HELO Plus firmware before 2.1.7 contains an information disclosure vulnerability that allows unauthenticated attackers to decrypt sensitive diagnostics bundles by exploiting a static AES passphrase embedded in obfuscated form within the firmware. Attackers can reverse engineer the publicly available firmware image to recover the shared passphrase and decrypt diagnostics export bundles retrieved from the unauthenticated diagnostics endpoint on any affected device, exposing highly sensitive server information.	7.5	More Details
CVE-2026-103271	Ghost versions from 4.0.0 before 6.63.0 contain a content API vulnerability that allows unauthenticated visitors to access gated post content. Attackers can bypass content restrictions by directly querying the content API to retrieve restricted posts without authentication.	7.5	More Details
CVE-2026-97244	Contributor Path Traversal in Creator LMS <= 1.2.19 versions.	7.5	More Details
CVE-2026-96348	Unauthenticated Broken Access Control in Bookly <= 28.2 versions.	7.5	More Details
CVE-2026-63292	Stack-based buffer overflow in mod_vhost_alias in Apache Software Foundation Apache HTTP Server through 2.4.68 on all platforms allows a remote client to cause a denial of service or potentially execute arbitrary code via an HTTP request with a Host header exceeding 8192 bytes when VirtualDocumentRoot uses a hostname format specifier and LimitRequestFieldSize is raised above the default. Users are recommended to upgrade to version 2.4.69, which fixes this issue.	7.5	More Details
CVE-2026-63045	Improper validation of FTP PASV reply address in mod_proxy_ftp in Apache Software Foundation Apache HTTP Server through 2.4.68 on all platforms allows, in forward proxy configurations, an untrusted FTP server to cause the proxy to open a data connection to an arbitrary third-party host via a crafted PASV response. Users are recommended to upgrade to version 2.4.69, which fixes this issue.	7.5	More Details
CVE-2026-59685	Out-of-bounds Write vulnerability in Apache HTTP Server on Windows while processing paths with 8.3 names that may grow when expanded. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	7.5	More Details
CVE-2026-56449	Out-of-bounds Write vulnerability in Apache HTTP Server's mod_proxy_html with crafted HTTP response bodies. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	7.5	More Details
CVE-2026-56153	Out-of-bounds Write vulnerability in Apache HTTP Server's mod_charset_lite. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	7.5	More Details
CVE-2026-	Unauthenticated Arbitrary File Download in NextGEN Gallery <= 4.5.0 versions.	7.5	More Details

94123			
CVE-2026-103913	The GeoDirectory plugin for WordPress is vulnerable to SQL Injection via the stored latitude/longitude coordinates of a listing in versions up to, and including, 2.8.186. This is due to insufficient escaping and the absence of numeric validation on coordinate values when a listing is saved, combined with the direct string interpolation of those values into a distance sub-expression in <code>geodir_gps_query_part()</code> that is later executed by the public <code>wp_ajax_nopriv_geodir_widget_listings</code> handler when a caller supplies <code>set_post=<pending-listing-id></code> and <code>sort_by=distance_asc</code> . 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.	7.5	More Details
CVE-2026-93428	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.13.1 This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to view privacy-restricted member profile field values — including fields explicitly configured as owner-only, members-only, or role-restricted — by querying the publicly accessible <code>wp_ajax_nopriv_um_get_members</code> endpoint. The nonce required by the endpoint ('um-frontend-nonce') is emitted to all unauthenticated visitors via <code>wp_localize_script</code> , meaning it provides no meaningful access control and any anonymous visitor can satisfy the endpoint's authentication requirements.	7.5	More Details
CVE-2026-101159	The WP Ultimate Review WordPress plugin before 2.4.4 does not properly sanitise and escape reviews submitted through its public review form, which is available to unauthenticated visitors, allowing them to perform Stored Cross-Site Scripting attacks against any user, including administrators, viewing a page displaying the review, when user reviews are enabled.	7.5	More Details
CVE-2026-97363	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks or brute-force attacks to gain unauthorized access.	7.5	More Details
CVE-2026-104861	<code>probe-image-size</code> gets image dimensions without downloading the entire file. Prior to 7.4.0, <code>lib/parse_sync/svg.js</code> and <code>lib/parse_stream/svg.js</code> use the searching regular expression <code>/<[_.:a-zA-Z0-9][^>]*>/</code> , which repeatedly scans to the end of input when attacker-controlled data contains many less-than characters without a closing greater-than character. The synchronous parser converts and scans the full supplied buffer without an input cap, while the streaming parser reparses the complete accumulated SVG prefix for every received chunk. The <code>probe.sync()</code> , <code>probe(stream)</code> , and <code>probe(url)</code> entry points can therefore block the Node.js event loop at full CPU, and attacker-controlled chunking can amplify the streaming cost. This issue is fixed in version 7.4.0.	7.5	More Details
CVE-2026-104057	Podgrab contains an unauthenticated denial-of-service vulnerability caused by unsynchronized concurrent access to shared maps (<code>activePlayers</code> and <code>allConnections</code>) in its WebSocket handler, where <code>Wshandler</code> and <code>HandleWebsocketMessages</code> goroutines read and write these maps without a mutex. A remote attacker can open multiple WebSocket connections to the <code>/ws</code> endpoint and send messages in a loop to trigger a Go runtime data race that crashes the process, causing a denial of service that requires operator intervention to restore service.	7.5	More Details
CVE-2026-102717	MQTT WebSocket setter ABI mismatch may disclose memory or cause a crash	7.5	More Details
CVE-2026-88394	WookTeam v1.6.6 and before is vulnerable to a Directory Traversal. The project task export endpoint <code>/api/project/task/export</code> downloads an arbitrary file from the server when the data parameter is supplied with a crafted JSON payload. The file value inside the JSON is concatenated directly into <code>storage_path(\$file)</code> without any path normalization or directory boundary check, so directory traversal (<code>../</code>) escapes the storage/ directory and <code>response()->download()</code> streams any file readable by the web server process.	7.5	More Details
CVE-2026-101161	The WP Ultimate Review WordPress plugin before 2.4.4 does not prevent unauthenticated users from storing crafted review content that makes the reviewed page fail with a fatal error on every subsequent visit, resulting in a persistent denial of service when the WP Ultimate Review WordPress plugin before 2.4.4's review display settings have never been saved.	7.5	More Details
CVE-2014-125130	CodeArt Google MP3 Audio Player plugin (<code>google-mp3-audio-player</code>) for WordPress through 1.0.11 contains an unauthenticated arbitrary file read vulnerability that allows remote attackers to retrieve sensitive files by supplying a path-traversal payload in the file parameter of <code>direct_download.php</code> . Attackers can request paths <code>../wp-config.php</code> without authentication to download configuration files containing database credentials and secret keys, leading to full site compromise. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-19.	7.5	More Details
CVE-			

2026-88392	Unimall v4 is vulnerable to Directory Traversal in FileUploadController.local(). This allows an attacker to execute arbitrary code.	7.5	More Details
CVE-2026-101160	The WP Ultimate Review WordPress plugin before 2.4.4 does not validate that a submitted review rating is numeric before storing it and later using it in numeric operations when rendering reviews, allowing unauthenticated users to make the reviewed content fail with a fatal error for all visitors until the review is removed (a persistent denial of service), when user reviews are enabled.	7.5	More Details
CVE-2026-104433	Mooncake transfer engine before 0.3.12 contains an out-of-bounds read vulnerability in the readString function of include/common.h that allows unauthenticated attackers to crash the service by sending a zero-length handshake frame. Attackers can connect to the handshake port listening on all interfaces and send an eight-byte frame to terminate the hosting process, such as an SGLang inference server.	7.5	More Details
CVE-2026-102504	Imager versions before 1.037 for Perl exit the process reading a raw image with an out-of-range raw_datachannels value in i_readraw_wiol. Nothing range-checks raw_datachannels. The line buffer is sized as the image width times the channel count with no overflow check, so a negative or very large count requests an excessive allocation. When it fails, Imager's allocator calls exit(3). Passing an untrusted raw_datachannels value to Imager->read() triggers an uncatchable exit.	7.5	More Details
CVE-2026-100514	Unauthenticated Insecure Direct Object References (IDOR) in REST API Log <= 1.7.2 versions.	7.5	More Details
CVE-2026-96823	Unauthenticated Arbitrary Content Deletion in Customer Reviews for WooCommerce <= 5.120.0 versions.	7.5	More Details
CVE-2023-54404	Zod schema-validation library through 4.6.5 contains an uncontrolled resource consumption vulnerability that allows attackers to exhaust memory by submitting a large array to an application using an array schema without a length constraint. Attackers can exploit the handleArrayResult parse logic in \$ZodArray, which accumulates every validation issue for each failing element with no cap or early termination, causing the process to allocate excessive issue objects and crash due to out-of-memory conditions.	7.5	More Details
CVE-2026-79896	Fortra BoKS Manager contains an out-of-bounds read vulnerability in the custom TLS ClientHello parser used by boks_portmux. A remote unauthenticated attacker can submit a malformed ClientHello and terminate boks_portmux. Although the daemon is normally restarted automatically, repeated requests can sustain the service interruption.	7.5	More Details
CVE-2026-94120	Unauthenticated Broken Access Control in GravityExport Lite for Gravity Forms <= 2.7.2 versions.	7.5	More Details
CVE-2026-103514	The WP 2FA WordPress plugin before 4.1.0 does not invalidate a time-based one-time passcode once it has been used, allowing an attacker who knows an account's password and has observed a valid code within its validity window to replay it and bypass two-factor authentication, including on administrator accounts.	7.5	More Details
CVE-2026-68496	The Smile parser in FasterXML jackson-dataformats-binary never invokes StreamReadConstraints.validateNameLength() when decoding JSON object property names, so the maxNameLength limit is not enforced for this format. SmileParser._handleLongFieldName() grows its internal name buffer through an unconstrained _growArrayTo() call and performs no length validation. An attacker who can have a Smile document parsed may therefore embed a single property name of unbounded length; the parser buffers the whole name in memory before returning it, whatever maxNameLength is configured to. Because StreamReadConstraints.maxDocumentLength is also disabled by default, nothing else bounds the name under default settings, so the only limits are the attacker's upload capacity and available heap, leading to memory exhaustion and denial of service. No privileges beyond the ability to submit data to a parsing endpoint are required, and exploitation needs only that the bytes reach SmileFactory parsing, directly or through an ObjectMapper configured with the Smile module. jackson-core's own JSON parsers enforce maxNameLength incrementally during name decoding; this gap is specific to the binary formats. maxNameLength and validateNameLength were introduced in jackson-core 2.16.0, so releases before 2.16.0 do not contain the constraint that is left unenforced. This issue is tracked together with the CBOR parser defect in the same vendor advisory, GHSA-3v8f-v6vx-fmrm, which covers both binary formats. The Smile parser defect (jackson-dataformats-binary issue #726) is CVE-2026-68496; the CBOR parser defect (issue #725) is assigned CVE-2026-68495.	7.5	More Details
CVE-	LightLLM through 1.2.0 mounts reinforcement learning control routes on the public HTTP API without		

2026-103270	authentication checks. Unauthenticated attackers can call endpoints like /pause_generation, /abort_request, /flush_cache, and /init_weights_update_group to disrupt inference operations and wedge workers on deployments started with --enable_rl.	7.5	More Details
CVE-2026-68495	The CBOR parser in FasterXML jackson-dataformats-binary never invokes StreamReadConstraints.validateNameLength() when decoding JSON object property names, so the maxNameLength limit is not enforced for this format. CBORParser._decodeLongerName() decodes a definite-length property name with no length check, and CBORParser._decodeChunkedName() delegates to the value-oriented _finishChunkedText() routine, which validates maxStringLength rather than maxNameLength. An attacker who can have a CBOR document parsed may therefore embed a single property name of unbounded length; the parser buffers the whole name in memory before returning it, whatever maxNameLength is configured to. Because StreamReadConstraints.maxDocumentLength is also disabled by default, nothing else bounds the name under default settings, so the only limits are the attacker's upload capacity and available heap, leading to memory exhaustion and denial of service. No privileges beyond the ability to submit data to a parsing endpoint are required, and exploitation needs only that the bytes reach CBORFactory parsing, directly or through an ObjectMapper configured with the CBOR module. jackson-core's own JSON parsers enforce maxNameLength incrementally during name decoding; this gap is specific to the binary formats. maxNameLength and validateNameLength were introduced in jackson-core 2.16.0, so releases before 2.16.0 do not contain the constraint that is left unenforced. This issue is tracked together with the Smile parser defect in the same vendor advisory, GHSA-3v8f-v6vx-fmrm, which covers both binary formats. The CBOR parser defect (jackson-dataformats-binary issue #725) is CVE-2026-68495; the Smile parser defect (issue #726) is assigned CVE-2026-68496.	7.5	More Details
CVE-2026-104845	Seroval facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. Prior to 1.6.3, deserializeTypedArray in fromJSON and fromCrossJSON trusts a deserialized source value as an ArrayBuffer and does not bound the serialized element count. An attacker can provide a small untrusted JSON object with a large length value, causing the array-like TypedArray constructor to synchronously allocate the selected number of elements and exhaust CPU or memory while starving the event loop. The offset check does not reject the crafted source because source.byteLength is undefined. DataView reaches a similar unchecked cast but throws rather than allocating, and the issue has no identified confidentiality or integrity impact. This issue is fixed in version 1.6.3.	7.5	More Details
CVE-2026-92121	In the WSS4J streaming (StAX) code, a signature reference using the WS-Security STR-Transform leaves an internal "inside signed content" flag permanently set. The WS-SecurityPolicy enforcer uses that flag to decide whether an element needs checking, so it stops evaluating SignedParts and SignedElements for the rest of the message. A policy requiring the SOAP Body to be signed is then satisfied even when the Body carries no signature, removing the protection against XML Signature Wrapping. Signature verification itself is unaffected. The DOM code is not affected. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4 which fix this issue.	7.5	More Details
CVE-2024-58388	Sharp (and Toshiba Tec rebranded) multifunction printers contain an unauthenticated local file inclusion vulnerability that allows remote attackers to read arbitrary files by manipulating the path parameter in the installed_emanual_down.html endpoint. Attackers can supply directory traversal sequences such as path=/manual/../.././.<path> to access files outside the intended manual directory, including /etc/passwd, coredump files containing credentials, and system configuration files. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-07-30.	7.5	More Details
CVE-2020-37278	Weaver e-Bridge contains an unauthenticated arbitrary file read vulnerability that allows remote attackers to access arbitrary files on the host system by supplying a file: URL to the downloadUrl parameter of the saveYZJFile endpoint. Attackers can exploit this flaw to read sensitive files such as /etc/passwd or configuration and credential files, and the same endpoint's support for http(s) URLs also enables server-side request forgery against internal network resources. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-17.	7.5	More Details
CVE-2026-103262	Tornado versions before 6.5.9 contain an unbounded memory accumulation vulnerability in CurlAsyncHttpClient that allows remote attackers to cause denial of service by sending a compressed response. Attackers can send a gzip-encoded decompression bomb that accumulates in memory without size limits, causing the application process to be killed by out-of-memory conditions.	7.5	More Details
CVE-2026-75823	The User Frontend WordPress plugin before 4.3.12 does not prevent tampering with the role assigned by its registration form, allowing unauthenticated users to register with a higher privileged role, such as Editor. This affects installations running a PHP build where the sodium extension is unavailable, and where a registration page has been configured. The administrator role cannot be obtained this way.	7.4	More Details
CVE-2026-	HCL BigFix Service Management is affected by an Insecure Communication vulnerability, which could allow an attacker with internal network access to intercept unencrypted HTTP traffic between backend	7.4	More Details

67105	services, enabling the extraction of sensitive data and potential man-in-the-middle (MitM) attacks.		
CVE-2026-15911	Confluent Kafka Python client's HashiCorp Vault KMS integration could allow a remote attacker to obtain sensitive information due to improper TLS certificate validation.	7.4	More Details
CVE-2026-80443	Improper certificate validation vulnerability in HAVELSAN Inc. Sef - AI Chatbot Platform allows Adversary in the Middle (AiTM). This issue affects Sef - AI Chatbot Platform: before 2.1. NOTE: The vendor was contacted and it was learned that the product is not supported.	7.4	More Details
CVE-2026-105294	Legcord 1.1.0 through 1.3.0 contains a configuration injection vulnerability that allows script in the Discord page to write any config key via the window.legcord.settings.setConfig bridge. Attackers exploiting a Discord XSS can set additionalArguments to persistently add --proxy-server and --ignore-certificate-errors switches, routing all client traffic through an interception proxy.	7.4	More Details
CVE-2026-105223	maclof kubernetes-client 0.17.0 before 0.32.0 disables TLS certificate verification in parseKubeconfig() and parseKubeconfigFile() when a kubeconfig lacks certificate-authority-data, ignoring insecure-skip-tls-verify. On-path attackers can impersonate the Kubernetes API server to capture Bearer tokens or Basic credentials and tamper with WebSocket or REST API traffic.	7.4	More Details
CVE-2026-103921	GraphQL Tools provides utilities for building, stitching, and mocking GraphQL schemas. Prior to 1.1.35, the executor-legacy-ws buildWSLegacyExecutor() function hardcodes TLS certificate rejection off for Node.js connections to wss:// endpoints. Applications using the executor directly, or url-loader with SubscriptionProtocol.LEGACY_WS, can therefore accept an attacker-controlled certificate when a network-positioned attacker intercepts the connection. Authentication material in connectionParams or headers can be disclosed, and subscription data can be modified. Browser WebSocket clients are unaffected because browsers enforce certificate validation. This issue is fixed in version 1.1.35.	7.4	More Details
CVE-2026-104435	Zebra zebra4 4.4.0 and zebra-script 6.0.0 fail to enforce a ZIP-244 consensus rule, accepting V5 transparent inputs signed with SIGHASH_SINGLE that lack a corresponding output. Attackers can broadcast crafted V5 transactions with more inputs than outputs that Zebra accepts but zcashd rejects, causing a network consensus split.	7.4	More Details
CVE-2026-105218	gopay before 1.5.119 disables TLS certificate verification in defaultClient() in pkg/xhttp/client.go, allowing man-in-the-middle attackers to impersonate payment provider APIs. Attackers can present any certificate to read merchant credentials, signatures and transaction data, and modify payment, refund and order query responses.	7.4	More Details
CVE-2026-105635	Plane is an open-source project management tool. Prior to 1.4.0, ProjectJoinEndpoint at GET /api/workspaces/{slug}/projects/{project_id}/join/{pk}/ uses permission_classes = [AllowAny] and returns the full ProjectMemberInvite record, including its email, token, and role, to unauthenticated callers. The corresponding POST endpoint checks only whether the submitted email matches project_invite.email and does not validate the invitation token. An attacker who knows the invitation UUID can discover the invited email, register an account with that email, and accept the invitation without receiving the original invite. This issue is fixed in 1.4.0.	7.4	More Details
CVE-2026-104437	Zebra before 4.4.0 contains a consensus divergence vulnerability in V5 transparent signature verification, computing a ZIP-244 digest for SIGHASH_SINGLE inputs lacking corresponding outputs instead of failing. Attackers can craft V5 transactions with fewer outputs than inputs that Zebra accepts and templates via getblocktemplate, producing blocks zcashd rejects.	7.4	More Details
CVE-2026-102123	A Kiteworks appliance setup interface did not confine a user-supplied file path to its intended directory, which could allow an unauthenticated attacker to write a file to any location writable by the affected service account, potentially compromising the integrity of the appliance or rendering it unavailable until an operator intervenes. Exploitation requires network access to the affected interface, which is not reachable on a fully configured appliance in its default configuration; reaching it depends on either the transient window while an appliance is first being provisioned or a non-default appliance configuration.	7.4	More Details
CVE-2026-105216	go-micro before 6.0.0 contains an improper certificate validation vulnerability that allows network attackers to impersonate services because the shared TLS helper sets InsecureSkipVerify to true by default. Man-in-the-middle attackers can present any certificate to intercept or modify gRPC transport, HTTP and RabbitMQ broker, and Consul or etcd registry traffic, including authentication tokens and credentials.	7.4	More Details
CVE-2026-105221	The gist RubyGem before 6.1.0 contains an improper certificate validation vulnerability that allows on-path attackers to intercept HTTPS traffic because http_connection in lib/gist.rb sets VERIFY_NONE. Attackers can present any certificate to read or modify GitHub API traffic, stealing OAuth tokens and login credentials to read and modify the victim's gists.	7.4	More Details

CVE-2026-105222	The alexpechkarev/google-maps Laravel package through 12.16 disables TLS certificate verification by default because the bundled config sets ssl_verify_peer to FALSE, which is passed to CURLOPT_SSL_VERIFYPEER. On-path attackers can present any certificate to intercept Google Maps web-service requests, steal the API key from the query string, and tamper with responses.	7.4	More Details
CVE-2026-97212	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	7.3	More Details
CVE-2026-102909	A vulnerability was identified in SourceCodester Online Reviewer Management System 1.0. Impacted is an unknown function of the file /reviewer_0/admins/assessments/examproper/btn_functions.php. The manipulation of the argument access_code leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-105169	A security flaw has been discovered in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. This impacts an unknown function of the file delivery/delivery.php of the component Take Order Handler. The manipulation of the argument order_id/delivery_person_id results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105170	A weakness has been identified in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. Affected is an unknown function of the file admin/signup.php of the component Admin Signup. This manipulation of the argument sign causes missing authentication. The attack can be initiated remotely. The exploit has been made available to the public and could 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 project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-103286	Ghost versions from 2.21.0 before 6.56.0 contain a privilege escalation vulnerability in the notifications system that allows low-privilege staff users to escalate to higher-privilege staff roles. Attackers with low-privilege staff access can exploit the notifications system to gain elevated privileges without proper authorization checks.	7.3	More Details
CVE-2026-105167	A vulnerability was determined in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. The impacted element is an unknown function of the file admin/donate.php. Executing a manipulation of the argument location can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-102262	Newell Brands DYMO ID 1.5.1.71 resolves its plugin Modules directory relative to the process working directory. An attacker could store a job file alongside malicious modules / DLL that sets the process working directory to the job file's folder when a victim clicks on the file, resulting in code execution at the victim's privilege level. Fixed in 1.6.0.	7.3	More Details
CVE-2026-102874	A vulnerability was identified in HKUDS AnyTool 0.1.0. Affected is the function subprocess.run of the file anytool/local_server/main.py of the component Execute Endpoint. The manipulation of the argument command/shell leads to os command 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-2026-105166	A vulnerability was found in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. The affected element is the function insert of the file fooddonateform.php of the component Food Donation Form. Performing a manipulation of the argument image-choice results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-	Path traversal / arbitrary file write in oc-mirror's operator catalog image extraction. When mirroring operator catalogs using either the legacy v1 path (--v1) or the OCI feature path (--use-oci-feature), oc-	7.3	More

101295	mirror extracts tar entries from catalog image layers without validating that file paths resolve within the intended destination directory.		Details
CVE-2026-102908	A vulnerability was determined in SourceCodester Online Reviewer Management System 1.0. This issue affects some unknown processing of the file /reviewer_0/admins/assessments/examproper/questions-view.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-105147	A vulnerability was determined in SciPhi-AI R2R up to 3.6.6. This affects an unknown part of the component JWT Secret Handler. This manipulation of the argument DEFAULT_BCRYPT_SECRET_KEY/DEFAULT_NACL_SECRET_KEY causes hard-coded credentials. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-105172	A vulnerability was detected in itsourcecode Online Admission System 1.0. Affected by this issue is some unknown functionality of the file /login1.php. Performing a manipulation of the argument User results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-103536	A vulnerability was identified in ZongXR Supermarket 1.0.0.0. Affected by this vulnerability is the function OrderController.addOrder of the file order/src/main/java/com/supermarket/order/controller/OrderController.java of the component save Endpoint. Such manipulation of the argument userId leads to missing authentication. The attack can be executed 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-2026-103552	Stack Overflow vulnerability in Apache Directory LDAP API. Before binding, a client can send a deeply nested search filter that overflows the stack in the server's decoder. This issue affects Apache Directory LDAP API: from 1.2.0 before 1.2.9. Users are recommended to upgrade to version 1.2.9, which fixes the issue.	7.3	More Details
CVE-2026-105290	A vulnerability was determined in feelec-yishu feelcrm-os 1.0.0. This affects an unknown part of the file App/Feelcrm/Index/Controller/GoogleController.class.php of the component getCurlData Endpoint. Executing a manipulation of the argument url can lead to server-side request forgery. It is possible to launch the attack 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.	7.3	More Details
CVE-2026-103530	A vulnerability was detected in decolua 9Router up to 0.5.55. The affected element is the function fetch of the file src/shared/utills/ssrfGuard.js of the component Search Endpoint. Performing a manipulation of the argument provider_options.baseUrl results in server-side request forgery. The attack can be initiated remotely. Applying a patch is the recommended action to fix this issue.	7.3	More Details
CVE-2026-105679	Ghost is a Node.js content management system. From 6.22.1 until 6.64.0, Ghost restricted the content type used to serve uploaded files to prevent browsers from executing them. On sites using the default local storage adapter, this restriction was not applied, so files uploaded by any staff user were served with a content type derived from their file extension. This could be used to host scripts on the site's domain, possibly resulting in compromise of other staff users' admin sessions. This issue is fixed in version 6.64.0.	7.3	More Details
CVE-2026-105133	A vulnerability was detected in Ahsay AhsayCBS up to 10.3.2. This affects the function checkSysPwd of the file com/ahsay/obs/api/ApiStructsAction.java of the component API. Performing a manipulation of the argument random results in improper authentication. It is possible to initiate the attack remotely. The exploit is now public and may be used. Upgrading to version 10.3.4 is able to mitigate this issue. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2026-105383	A vulnerability has been found in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. This impacts an unknown function of the file php/controller.php. Such manipulation of the argument transaction_idS leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105253	A vulnerability was determined in itsourcecode Online Admission System Project 1.0. This issue affects some unknown processing of the file /admin/login1.php. This manipulation of the argument User causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
	A vulnerability has been found in rhukster dom-sanitizer up to 1.0.15. The affected element is the function url of the file src/DOMSanitizer.php of the component SVG Sanitization. Such manipulation		

CVE-2026-103687	leads to incomplete blacklist. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.16 is sufficient to fix this issue. The name of the patch is 139c46c3d7c9bc81542b7b5a58d5cde5d0e0195a. Upgrading the affected component is recommended.	7.3	More Details
CVE-2026-105175	A vulnerability was found in SourceCodester Drug Recommendation System 1.0. This issue affects some unknown processing of the file /Auth/add_student.php of the component Student Registration. The manipulation of the argument cmdschool 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-2026-105382	A flaw has been found in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. This affects the function update_subaccount of the file php/controller.php of the component Account Administration. This manipulation of the argument user_id causes improper authorization. Remote exploitation of the attack is possible. The exploit has been published and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105158	A vulnerability was detected in RainyGao DocSys up to 2.02.85. The impacted element is the function BaseController.createDBForMysql of the file BaseController.java of the component Database Management. The manipulation of the argument url results in sql injection. The attack can be executed 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-2026-105149	A security flaw has been discovered in mooSocial up to 3.2.4. This issue affects some unknown processing of the file /stores/all-products. Performing a manipulation of the argument rating results in sql injection. The attack may 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-2026-105148	A vulnerability was identified in SciPhi-AI R2R up to 3.6.6. This vulnerability affects unknown code of the file py/shared/abstractions/llm.py of the component Retrieval Completion API Endpoint. Such manipulation of the argument generation_config.api_base leads to server-side request forgery. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-105307	A vulnerability was detected in Casdoor up to 3.161.1. Affected is the function ApiFilter of the file routers/authz_filter.go of the component API Endpoint. Performing a manipulation results in missing authentication. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-105238	A flaw has been found in ChatGPTNextWeb NextChat up to 2.16.1. This vulnerability affects the function proxyHandler of the file app/api/proxy.ts of the component Proxy Fallback Handler. This manipulation of the argument x-base-url causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	7.3	More Details
CVE-2026-102913	A security flaw has been discovered in SourceCodester Car Driving School Management System 1.0. Impacted is an unknown function of the file /classes/Master.php?f=save_enrollment. The manipulation results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-103232	A weakness has been identified in AdithyaYelloju Restaurant-Management-System up to 7f0e7e84255e8fcfd488e83f8f91451bbbff6b9c. This affects the function mysqli_query of the file admin/table_booking.php. This manipulation of the argument Name causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105183	A weakness has been identified in itsourcecode Online Admission System 1.0. The affected element is an unknown function of the file /admin/confirm.php. This manipulation of the argument schedid 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.	7.3	More Details
CVE-2026-105184	A security vulnerability has been detected in itsourcecode Online Admission System 1.0. The impacted element is an unknown function of the file /admin/criteria.php. Such manipulation of the argument ID 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-2026-105643	Ghost is a Node.js content management system. From version 6.34.0 until 6.67.0, embed cards in the Ghost editor could bypass protections against stored cross-site scripting. Any staff user, including Contributors, could store scripts in post content that ran when another staff user opened the post in the editor, potentially compromising that user's admin session. Self-hosted sites should leave the new security.embedPreviewUrl configuration option at its default value. This issue is fixed in version 6.67.0.	7.3	More Details
CVE-2026-105247	A vulnerability was determined in SourceCodester Online Reviewer Management System 1.0. The affected element is an unknown function of the file /reviewer_0/admins/assessments/Subject/btn_functions.php?action=course. Executing a manipulation of the argument Subject can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-105232	A flaw has been found in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. The impacted element is an unknown function of the file delivery/deliverysignup.php of the component Registration Page. This manipulation of the argument username/email/location causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-104123	A vulnerability was detected in SourceCodester Online Reviewer Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /reviewer_0/admins/assessments/activities/btn_functions.php?action=activity. The manipulation of the argument Title results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-104120	A security vulnerability has been detected in modelcontextprotocol mcp-server-fetch and mcp-server-everything up to 2026.6.4. Affected is the function fetch_url of the file mcp_server_fetch/server.py of the component Fetch Tool. The manipulation of the argument url/path leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	7.3	More Details
CVE-2026-47496	NVIDIA GPU Display Driver for Linux contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where a guest VM user may cause an out-of-bounds write by sending a specially crafted RPC call to the host. A successful exploit of this vulnerability might lead to escalation of privileges, data tampering, and denial of service.	7.3	More Details
CVE-2026-105386	A vulnerability was identified in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. Affected by this issue is the function get of the file print.php. The manipulation of the argument transaction_id leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-102910	A security flaw has been discovered in SourceCodester Online Reviewer Management System 1.0. The affected element is an unknown function of the file /reviewer_0/admins/assessments/examproper/exam-delete.php. The manipulation of the argument test_id results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-105185	A vulnerability was detected in itsourcecode Online Admission System 1.0. This affects an unknown function of the file /admin/examinee.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-105387	A security flaw has been discovered in girishsaraf Online-Appointment-Booking-System up to f427b4757128ca253d33d0cc4e87bbb9c999a4d5. This affects the function mysqli_query of the file cover.php of the component Patient Login Handler. The manipulation of the argument uname/psw results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-47580	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where an attacker could cause a missing authorization issue. A successful exploit of this vulnerability might lead to information disclosure and data tampering.	7.3	More Details

CVE-2026-105231	A vulnerability was detected in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. The affected element is an unknown function of the file admin/signup.php of the component Admin Registration. The manipulation of the argument email/username/location results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105230	A security vulnerability has been detected in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. Impacted is an unknown function of the file delivery/deliverymyord.php. The manipulation of the argument delivery_person_id/order_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105229	A weakness has been identified in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. This issue affects some unknown processing of the file signup.php of the component User Registration Endpoint. Executing a manipulation of the argument email/name/gender can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-51917	FinRobot v1.0.0 is vulnerable to Code Injection in CodingUtils.modify_code.	7.3	More Details
CVE-2026-105182	A security flaw has been discovered in SourceCodester Online Reviewer Management System 1.0. Impacted is an unknown function of the file /reviewer_0/admins/assessments/activities/btn_functions.php?action=update. The manipulation of the argument Title 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-2026-104413	Ghost from 5.94.0 before 6.64.0 contains a stored cross-site scripting vulnerability that allows staff users, including Contributors, to host arbitrary HTML by abusing bookmark card image fetching. Attackers can create bookmark cards that store non-image files from external websites as icons or thumbnails to compromise other staff users' admin sessions.	7.3	More Details
CVE-2026-73637	Use after free in mod_auth_digest in Apache Software Foundation Apache HTTP Server before 2.4.69 on all platforms allows an unauthenticated remote client to cause authentication state corruption via concurrent Digest authentication requests when AuthDigestNcCheck is enabled or AuthDigestNonceLifetime is set to 0. Users are recommended to upgrade to version 2.4.69, which fixes this issue.	7.3	More Details
CVE-2026-104637	A weakness has been identified in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. The affected element is the function add_patient/add_physician/add_account/update_account/update_subaccount/edit_physician/edit_patient of the file php/controller.php. Executing a manipulation of the argument img can lead to unrestricted upload. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105651	Ghost is a Node.js content management system. From 5.94.0 until 6.64.0, when creating a bookmark card, Ghost could store non-image files fetched from an external website as bookmark icons or thumbnails. This allowed any staff user, including Contributors, to host arbitrary HTML on the site's domain, possibly resulting in compromise of other staff users' admin sessions. This issue is fixed in version 6.64.0.	7.3	More Details
CVE-2026-105649	Ghost is a Node.js content management system. From 4.22.0 until 6.65.0, SVG media thumbnails and SVG images uploaded with a non-SVG file extension were stored without sanitization. This allowed any staff user, including Contributors, to host scripts on the site's domain, possibly resulting in compromise of other staff users' admin sessions. This issue is fixed in version 6.65.0.	7.3	More Details
	Ghost from 6.22.1 before 6.64.0 contains a stored cross-site scripting vulnerability that allows staff		

CVE-2026-104411	users to host scripts by uploading files served with extension-derived content types on the default local storage adapter. Attackers can upload script-bearing files to the site's domain to compromise other staff users' admin sessions.	7.3	More Details
CVE-2026-105392	A vulnerability has been found in Lybba Django-Vue-Lyadmin up to 3.2.12. The impacted element is an unknown function of the file backend/application/settings.py of the component JWT Signing. The manipulation of the argument SECRET_KEY leads to use of hard-coded cryptographic key . Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The project maintainer explains: "The issue with this key is described in the documentation. Developers need to manually change their keys before deployment."	7.3	More Details
CVE-2026-103230	A vulnerability was determined in AdithyaYelloju Restaurant-Management-System up to 7f0e7e84255e8fcfd488e83f8f91451bbbff6b9c. Impacted is the function mysqli_query of the file User/ord.php of the component Order Placement. Executing a manipulation of the argument id/name can lead to sql injection. The attack can be launched 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.	7.3	More Details
CVE-2026-105246	A vulnerability was found in SourceCodester Online Reviewer Management System 1.0. Impacted is an unknown function of the file /reviewer_0/admins/assessments/Subject/btn_functions.php?action=update. Performing a manipulation of the argument Subject results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-103229	A vulnerability was found in AdithyaYelloju Restaurant-Management-System up to 7f0e7e84255e8fcfd488e83f8f91451bbbff6b9c. This issue affects the function mysqli_query of the file admin/delete1.php of the component Unauthenticated Action Script. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2019-25777	YAML versions before 1.27_001 for Perl allow a loaded perl/glob document to replace any package variable, which can lead to arbitrary code execution. A perl/glob document names a package and a symbol, and supplies the value assigned to it. Nothing restricts the name, so the target can be @INC or YAML's own load options. A perl/glob document that sets \$YAML::LoadCode or \$YAML::UseCode turns on code loading, which is off by default, for every later Load() in the process. A perl/code document is then passed to a string eval, so an attacker who supplies two documents to separate Load() calls in one process can execute arbitrary Perl code.	7.3	More Details
CVE-2026-105385	A vulnerability was determined in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. Affected by this vulnerability is an unknown functionality of the file transaction_details.php. Executing a manipulation of the argument transaction_id can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-103278	Ghost versions 5.8.0 before 6.34.0 contain an input validation vulnerability in the admin iframe that allows attackers to take over staff user accounts. Attackers with content publishing privileges can craft malicious pages that, when visited by active staff users, enable account takeover through improper input validation.	7.3	More Details
CVE-2026-104609	A weakness has been identified in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. This affects the function get of the file edit_accounts.php. This manipulation of the argument user_id/patient_id/physician_id/discounts_id/services_id causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-105384	A vulnerability was found in UNION HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. Affected is an unknown function of the file patient_info.php. Performing a manipulation of the argument patient_id results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details

CVE-2026-103231	A vulnerability was identified in AdithyaYelloju Restaurant-Management-System up to 7f0e7e84255e8fcfd488e83f8f91451bbbff6b9c. The affected element is the function mysqli_query of the file User/cancel.php of the component Order Cancellation. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-97341	The Visitor Traffic Real Time Statistics plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via 'X-Real-IP' HTTP Header in all versions up to, and including, 8.16 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires no authentication, no nonce, and no capability — the wp_ajax_nopriv_ahcfree_track_visitor endpoint accepts the forged X-Real-IP header from any unauthenticated HTTP request and stores the entity-encoded payload verbatim in the database.	7.2	More Details
CVE-2026-103426	The Relevanssi Premium plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_rt' parameter in all versions up to, and including, 2.31.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the click-tracking and logging feature to be activated in the plugin settings, and exploitation is trivially accessible to unauthenticated users because a valid _rt_nonce is publicly emitted on every search-results page.	7.2	More Details
CVE-2026-93875	The JetAppointment plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'friendlyTime' parameter in all versions up to, and including, 2.5.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload is stored in the wp_jet_appointments_meta table via the unauthenticated jet_engine_form_booking_submit endpoint and executes in the administrator's browser when the appointment details popup is opened in the WordPress admin panel.	7.2	More Details
CVE-2026-95817	The DoFollow Case by Case plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 3.6.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Comment moderation delays but does not prevent exploitation — once an administrator approves the visually innocuous comment, the stored payload executes in the browser of every subsequent visitor to the affected post.	7.2	More Details
CVE-2026-55231	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to version 1.0.8.6, a flawed central path sanitizer lets an authenticated admin-panel user who holds backup access (default role site_admin or higher) read and delete arbitrary files on a server. An attacker can recover database credentials from config/db.php, read host files such as /etc/passwd, and delete config/db.php to push a site back into install mode for a full takeover. This issue has been patched in version 1.0.8.6.	7.2	More Details
CVE-2026-103082	Server-Side Request Forgery (SSRF) vulnerability in LA-Studio LA-Studio Element Kit for Elementor lastudio-element-kit allows Server Side Request Forgery.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.6.2.	7.2	More Details
CVE-2026-95670	The No External Links plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Log URL via /goto/{base64} Redirect in all versions up to, and including, 5.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when the administrator has enabled the 'Link Encoding: Base64' option in the plugin settings.	7.2	More Details
CVE-2026-87091	The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Settlement Notification Parameters in all versions up to, and including, 2.12.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The IPN endpoint accepts the 'rel' and 'option' parameters with no authentication, nonce validation, or signature verification, meaning any unauthenticated attacker can directly submit malicious payloads that are stored and later rendered in the administrator's settlement error log view.	7.2	More Details
CVE-2026-100182	The Download Monitor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Cross-Origin postMessage to Admin Editor in all versions up to, and including, 5.2.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the attacker to trick an authenticated Administrator into visiting an attacker-controlled page that targets an open Download edit screen, after which the payload is persisted unfiltered via the Administrator's unfiltered_html capability and later emitted verbatim to the frontend by the	7.2	More Details

	[download_data] shortcode's unescaped post_content render path.		
CVE-2026-53964	Document Merge Service is a document template merge service providing an API to manage templates and merge them with given data. Prior to version 9.1.0, a remote code execution (RCE) via server-side template injection (SSTI) allows for user supplied code to be executed in the server's context where it is executed as the document-merge-server user with the UID 901 thus giving an attacker considerable control over the container. The vulnerability is limited to XLSX templates, where the xltpl library uses a npn-sandboxed Jinja environment for the processing of the template. This issue has been patched in version 9.1.0.	7.2	More Details
CVE-2026-96650	The Strong Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'platform_user_photo' Custom Field in all versions up to, and including, 3.3.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that an administrator has added custom text fields named 'platform' and 'platform_user_photo' to a public testimonial submission form, as the plugin does not reserve those internal metadata keys.	7.2	More Details
CVE-2026-96575	The Transliterator - Multilingual and Multi-script Text Conversion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via Predictable {rstr_keep} Placeholder in all versions up to, and including, 2.5.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload survives WordPress comment save-time sanitization because the tags and attributes used (such as a[title] and code) are permitted by the core commentkses allow-list, and the literal characters comprising the plugin's shortcode markers and placeholder tokens are not stripped.	7.2	More Details
CVE-2026-102772	The CMB2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '<textarea_code field id>' (e.g. kl_code, kl_post_code)' parameter in all versions up to, and including, 2.13.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The front-end save path requires only a CMB2 box nonce, which is emitted to all visitors including unauthenticated guests via a simple GET request, making the attack trivially reachable without any credentials on sites that expose a public CMB2 form writing a textarea_code field.	7.2	More Details
CVE-2026-96564	The SEOPress - AI SEO Plugin & On-site SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Author Display Name in all versions up to, and including, 10.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the 'Track Authors' custom dimension to be configured in the plugin's Google Analytics 4 or Matomo settings, and the attacker must be able to publish public singular content (e.g., via bbPress forum topics) so that the injected display name is rendered in the tracking script.	7.2	More Details
CVE-2026-93430	The GD Rating System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'title' and 'url' Render Args in gdrts_live_handler AJAX in all versions up to, and including, 3.7.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Although the AJAX action requires a per-item nonce, that nonce is publicly emitted in the page's <script class="gdrts-rating-data"> JSON block on every page rendering the rating item, making it obtainable by any unauthenticated visitor and therefore not an authentication barrier.	7.2	More Details
CVE-2026-104471	YesWiki before 4.6.7 contains an unrestricted file upload vulnerability that allows authenticated admins to write remote files into the web-accessible files/ directory via Bazar CSV import preview. Attackers can import a CSV whose file or image field references a remote .php URL, which is saved without extension checks and executed as server-side code.	7.2	More Details
CVE-2026-92144	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'postdata-1[post-custom]' Parameter in all versions up to, and including, 1.57.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The required form submission nonce is freely obtainable by unauthenticated users via the publicly accessible wp_ajax_nopriv_forminator_get_nonce endpoint, making the full attack chain exploitable without any authentication or prior account.	7.2	More Details
CVE-2026-100107	The Kubio AI Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 2.9.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details

CVE-2026-102565	The BA Book Everything plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'booking_service_qty' parameter in all versions up to, and including, 1.8.28 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires that an administrator or other privileged user opens the injected order record in the plugin's wp-admin order management area, which is the plugin's ordinary order-review workflow.	7.2	More Details
CVE-2026-96566	The Newsletter – Send awesome emails from WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'np1' Custom Field Parameter in all versions up to, and including, 9.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The subscription endpoint (na=sa) requires no nonce, no capability check, and no CAPTCHA, and the payload can be smuggled past email-address validation by embedding the {profile_1} placeholder in the local part of the submitted address, since WordPress's is_email() permits curly braces there.	7.2	More Details
CVE-2026-96567	The MW WP Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_id' parameter in all versions up to, and including, 5.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The CSRF gate protecting form submission (MW_WP_Form_Csrf) is bypassable by any unauthenticated visitor who first loads the public form page to obtain a valid double-submit cookie, leaving no effective barrier to storing malicious payloads.	7.2	More Details
CVE-2026-101928	The Magic Tooltips For Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author' parameter in all versions up to, and including, 1.0.34 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because the plugin's esc_html filter callback decodes HTML-entity-encoded payloads (e.g. those containing '<tip>') back into live HTML, meaning an entity-encoded script payload submitted as a comment author name — which bypasses sanitize_text_field — is rendered as executable markup when an administrator views wp-admin/edit-comments.php.	7.2	More Details
CVE-2026-85679	The Extendify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'styles.blocks' Block Type Key in all versions up to, and including, 3.1.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because registerIncoming() is hooked on rest_request_before_callbacks and runs before WordPress evaluates the route's permission_callback, meaning any unauthenticated POST, PUT, or PATCH request to a /wp/v2/global-styles route can trigger the vulnerable code path.	7.2	More Details
CVE-2026-101888	The Prime Mover plugin for WordPress before 2.2.1 contains a Zip Slip path traversal vulnerability that allows authenticated administrators to write arbitrary files outside the intended extraction directory during migration ZIP import. Attackers can craft ZIP entry names with traversal sequences processed by computeExtractionParameters() and resumableZipExtractor() in utilities/PrimeMoverSystemCheckUtilities.php to write attacker-controlled content to arbitrary filesystem locations, potentially achieving remote code execution if the written files are interpreted by the web environment.	7.2	More Details
CVE-2026-105126	LaraDashboard before 1.4.8 contains an improper privilege management vulnerability that allows authenticated Admin users to escalate to Superadmin by editing or renaming roles. Attackers with role.edit can rename their role to Superadmin or grant user.login_as permissions to take over accounts and reach core upgrade and module installation functions for code execution.	7.2	More Details
CVE-2026-87920	The W3 Total Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via Output-Buffer Regex Rewrite in all versions up to, and including, 2.10.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is only exploitable when the 'Remove query strings from static resources' option is enabled in W3 Total Cache, as mutate_url() must strip the '?' delimiter and everything following it — including the closing quote of the outer attribute — to break the attribute boundary.	7.2	More Details
CVE-2026-97660	The WPC Product Options for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via wpcpo-* Array Key via Multipart Field Name in all versions up to, and including, 4.0.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is exploitable via guest checkout without authentication because the malicious payload is embedded in a multipart Content-Disposition field name beginning with 'wpcpo-', which PHP's RFC1867 parser preserves byte-for-byte and stores into order item meta.	7.2	More Details

CVE-2026-14995	The Autooptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REQUEST_URI Path in all versions up to, and including, 3.1.15.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the Critical CSS feature to be active with a valid API key configured, as this is the precondition for unauthenticated frontend requests to trigger queue entries via ao_ccss_enqueue().	7.2	More Details
CVE-2026-90438	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Paragraph Text (RTE) Field Submission in all versions up to, and including, 3.15.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when the targeted Paragraph Text field has the Rich Text Editor (RTE) option enabled.	7.2	More Details
CVE-2026-85235	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Rich-Text Textarea Field in all versions up to, and including, 1.57.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires an administrator to open the stored submission entry in the Forminator Entries view and interact with the planted link, at which point WordPress core's jQuery-based click handler on <code>`.contextual-help-tabs a`</code> evaluates the entity-decoded href as HTML, firing the attacker's payload in the administrator's authenticated wp-admin session.	7.2	More Details
CVE-2026-92244	The PDF Invoices & Packing Slips for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Billing First Name / Last Name / Company Fields in all versions up to, and including, 5.16.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload survives initial storage because WooCommerce's <code>sanitize_text_field()</code> and <code>wc_clean()</code> do not strip entity-encoded strings containing no literal <code>'<'</code> character, allowing unauthenticated guest-checkout orders to plant the malicious content.	7.2	More Details
CVE-2026-96573	The Appointment Hour Booking – Booking Calendar plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via Booking Form Single-Line Field via Schedule Calendar List Renderer in all versions up to, and including, 1.5.97 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the <code>'list_readmore_numberofwords'</code> Other Parameters setting to be configured with a positive integer value; the default value of 0 bypasses the decode-and-truncate branch entirely and is not exploitable through this sink.	7.2	More Details
CVE-2026-92977	The Real Cookie Banner: GDPR & ePrivacy Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment in all versions up to, and including, 5.3.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Malicious script payloads placed in the title attribute of an anchor tag survive WordPress's comment kses filter at save time, as the payload is only promoted to executable HTML attributes when the plugin's page-wide regex strips the closing quote delimiter at render time; exploitability is therefore subject to the standard comment moderation workflow before the comment is publicly displayed.	7.2	More Details
CVE-2026-96813	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Mark on Map Longitude/Latitude Fields in all versions up to, and including, 1.15.47 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-10026	The CTX Feed Pro plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 7.6.12. This is due to insufficient input validation on the 'Feed Config' field which is passed directly to the <code>eval()</code> function. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute arbitrary PHP code on the server.	7.2	More Details
CVE-2026-94390	Editor PHP Object Injection in Hide Shipping Method For WooCommerce <= 1.5.4 versions.	7.2	More Details
CVE-2026-97661	The Business Essentials for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'gateway' Form Field in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the Payments module to be enabled and a form to be configured to accept both PayPal and Stripe as payment gateways.	7.2	More Details

CVE-2026-93367	The Visitors Traffic Real Time Statistics Pro plugin for WordPress is vulnerable to unauthenticated stored Cross-Site Scripting in all versions up to, and including, 11.22 via the page_title parameter of the ahcpro_track_visitor AJAX action. The action is registered for logged-out callers (wp_ajax_nopriv_ahcpro_track_visitor) and stores \$_POST['page_title'] with NO sanitization, keeping it raw in the ahc_title_traffic.til_page_title column. When an administrator opens the plugin's dashboard, the 'Traffic by Title' DataTable renders that stored value as innerHTML without output escaping, executing arbitrary JavaScript. This makes it possible for unauthenticated attackers to inject web scripts that run in an administrator's session.	7.2	More Details
CVE-2026-93889	The Mail logging – WP Mail Catcher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via PHPMailer 'wp_mail_failed' Error Message in all versions up to, and including, 2.1.12 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires a separately installed plugin, such as Contact Form 7, that passes unauthenticated user-controlled input into mail fields whose content PHPMailer will include in its failure error message.	7.2	More Details
CVE-2026-96270	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_id' parameter in all versions up to, and including, 2.13.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload is stored in the registering user's 'submitted' usermeta via update_user_meta() and is only triggered when an administrator opens the affected user record in the wp-admin Users modal, which inserts the unescaped output via jQuery .html().	7.2	More Details
CVE-2026-97663	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Author Name in all versions up to, and including, 5.122.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the image attachment feature (ivole_attach_image) to be enabled, which allows unauthenticated attackers to both submit a review with an entity-encoded malicious author name and upload an attached image via the publicly accessible wp_ajax_nopriv_cr_upload_local_images_frontend endpoint.	7.2	More Details
CVE-2026-96561	The AI Engine – The Chatbot, AI Framework & MCP for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.8.0 This is due to a chain of missing input neutralization and output escaping across the /mwai-ui/v1/chats/submit REST endpoint, the PHP error-log parser (MeowKit_MWAI_Helpers::php_error_logs), the Advisor task (Meow_MWAI_Modules_Advisor::run_advisor), and the Advisor dashboard widget (advisor_metabox): the server-parameter denylist in chat_submit strips only exact key names such as 'model' while convert_keys() later canonicalizes 'model_' back to 'model', allowing an unauthenticated caller to place an attacker-controlled string (including CR/LF) into \$query->model; final_checks() throws an Exception whose message embeds that raw string, and the non-streaming, non-admin catch branch writes it to the PHP error log unmodified — creating a forged log line that the plugin's own parser subsequently returns as recent PHP-error content; run_advisor() then appends that content verbatim to the AI prompt (indirect prompt injection — CWE-1427), the returned JSON is stored in the mwai_advisor_data option with no schema validation or HTML sanitization, and advisor_metabox() concatenates the resulting 'title' and 'description' values directly into the WordPress dashboard widget without esc_html(), wp_kses(), or equivalent escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the WordPress dashboard.	7.2	More Details
CVE-2026-56589	HCL BigFix Service Management is affected by a Stored Cross-Site Scripting (XSS) vulnerability, which could allow an attacker to inject and store malicious scripts within the application that execute when a victim views the affected page, enabling session hijacking and the theft of sensitive data.	7.2	More Details
CVE-2026-103490	In JetBrains YouTrack before 2026.2.19422 privilege escalation was possible via user group links	7.2	More Details
CVE-2026-97641	The Relevanssi – A Better Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 4.28.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when the administrator has configured a non-empty value for the "Allowable tags in excerpts" setting, such as the default example value of <p><a>, as the prefix-matching regex must have an allowable tag whose name is a prefix of the injected tag name.	7.2	More Details

CVE-2026-97342	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'choice' Post Meta via Insert/Update Post Action in all versions up to, and including, 3.6.5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload is submitted via the unauthenticated wp_ajax_nopriv_jet_form_builder_submit endpoint, stored verbatim into post meta through the Insert/Update Post action, and later rendered unescaped by the Select Field block template when the get_from_db option generator copies raw meta values into option value attributes and label content.	7.2	More Details
CVE-2026-103766	ClipBucket v5 through 5.5.3-#197 contains an sql injection vulnerability that allows authenticated users with ad_manager_access permission to inject SQL via the delete parameter in admin_area/ads_manager.php. Attackers can supply time-based blind payloads concatenated into AdsManager::DeleteAd queries to extract user credentials and emails or modify and delete arbitrary records.	7.2	More Details
CVE-2026-104418	Ghost from 6.10.3 before 6.64.0 contains a remote code execution vulnerability that allows authenticated administrators to run code by abusing theme translation file loading. Attackers with administrator access can upload a crafted theme containing malicious translation files to execute arbitrary code on the Ghost server.	7.2	More Details
CVE-2026-96871	The Mang Board plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data_type' parameter in all versions up to, and including, 2.4.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is exploitable on any board configured with the default write_level=0 (guest posting) and editor_type=N settings, which are the out-of-the-box defaults for newly created boards.	7.2	More Details
CVE-2026-96578	The GSpeech TTS – WordPress Text To Speech Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 3.22.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This mXSS-style transform bypasses WordPress comment kses sanitization because the payload is stored using only kses-allowed tags and attributes; the malicious event handlers and style fragments become active only when the plugin's output-buffer callback rewrites the rendered HTML at request time.	7.2	More Details
CVE-2026-97336	The CMB2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'file_list' Field Type in all versions up to, and including, 2.13.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when an integrating plugin or theme registers a file_list field on a publicly accessible front-end form or a user meta box, as CMB2 is a developer library and does not expose these fields by default.	7.2	More Details
CVE-2026-93756	The Smash Balloon Social Post Feed – Simple Social Feeds for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Facebook Comment Message via v-html in Admin Builder Preview in all versions up to, and including, 4.13.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute whenever an administrator accesses the feed builder preview page. This attack requires only a Facebook account to post a comment on the connected Facebook Page, with no WordPress credentials needed; additionally, the use of v-show rather than v-if means injected HTML — including onerror handlers — is evaluated in the DOM even when the comment section is not visually displayed. When combined with the lack of URL validation in the cff_install_addon AJAX handler (admin/addon-functions.php), an injected script running in an administrator's session can trigger arbitrary plugin installation from an attacker-controlled URL, which may result in server-side code execution.	7.2	More Details
CVE-2026-102150	A function in the Kiteworks Advanced Forms component was reachable without authentication. An unauthenticated attacker could potentially use it to carry out a limited set of internal service operations on the Kiteworks platform; it did not permit access to user accounts, stored files, or form submissions.	7.2	More Details
CVE-2026-94122	Editor PHP Object Injection in Responsive Slider Gallery <= 1.5.5 versions.	7.2	More Details
CVE-2026-102098	Kiteworks Core before version 9.5.0 is vulnerable to SQL Injection. A stored SQL injection vulnerability in a Kiteworks administrative reporting feature could allow an authenticated administrator to read sensitive data from the underlying database and to affect the availability of the service. Exploitation requires an existing, authenticated administrative account with access to the affected reporting function.	7.2	More Details
CVE-	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Remote Code Execution.		

2026-102097	Kiteworks Email Protection Gateway allowed an authenticated administrator to import configuration whose contents were not sufficiently validated before being processed. A crafted submission could potentially allow arbitrary commands to be executed on the affected gateway.	7.2	More Details
CVE-2026-97347	The Post Views Stats Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via User-Agent Header in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The plugin's only input filter is a substring blacklist for known bot signatures (e.g. 'bot', 'spider', 'crawler'), which can be trivially bypassed by crafting a User-Agent payload that omits those strings.	7.2	More Details
CVE-2026-102096	Kiteworks Core before version 9.5.0 is vulnerable to OS Command Injection that allows an authenticated administrator to upload a configuration package whose contents were not sufficiently validated before being processed. A crafted package could cause the underlying system to execute arbitrary operating-system commands, potentially with elevated privileges, on the affected appliance.	7.2	More Details
CVE-2026-103349	Deserialization of Untrusted Data vulnerability in Rymera Web Co Product Feed PRO for WooCommerce woo-product-feed-pro allows Object Injection.This issue affects Product Feed PRO for WooCommerce: from n/a through 13.5.7.	7.2	More Details
CVE-2026-102094	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to Unsafe Reflection and does not sufficiently restrict the code that the mail-processing pipeline could load from an imported rule configuration. An authenticated administrator with mail-rule configuration privileges could cause the gateway to load and execute code beyond the approved set of mail-processing components, potentially in the context of the mail-gateway service account.	7.2	More Details
CVE-2026-102093	Kiteworks Core before version 9.5.0 is vulnerable to Improper Privilege Management and does not correctly enforce restrictions on role assignment, which could allow an authenticated administrative user with limited, non-Sysadmin role-management permissions to elevate another user to full system-administrator privileges beyond those the administrative user was authorized to grant.	7.2	More Details
CVE-2026-102089	Kiteworks Email Protection Gateway before version 9.5.0 is vulnerable to a path traversal weakness in an administrative import function allowed an authenticated administrator to write files to arbitrary locations on the server. This could potentially be leveraged to execute arbitrary code on the underlying system.	7.2	More Details
CVE-2026-93624	Shop manager PHP Object Injection in Music Player for WooCommerce <= 1.9.1 versions.	7.2	More Details
CVE-2026-93771	Shop manager PHP Object Injection in Cost of Goods for WooCommerce <= 3.5.2 versions.	7.2	More Details
CVE-2026-97256	Editor PHP Object Injection in Page Builder by SiteOrigin <= 2.36.0 versions.	7.2	More Details
CVE-2026-102108	An authenticated administrator of Kiteworks Email Protection Gateway could submit a crafted serialized object to a cluster management interface that was deserialized without sufficient validation, potentially allowing arbitrary code execution in the context of the gateway service account. Exploitation requires an administrator account holding a specific queue-management privilege.	7.2	More Details
CVE-2026-94677	Shop manager PHP Object Injection in Kadence WooCommerce Email Designer <= 1.5.19.1 versions.	7.2	More Details
CVE-2026-96343	Custom role PHP Object Injection in WP ERP <= 1.17.9 versions.	7.2	More Details
CVE-2026-96344	Custom role PHP Object Injection in eCommerce Product Catalog <= 3.6.0 versions.	7.2	More Details
CVE-2026-96815	Custom role Privilege Escalation in Vitepos <= 3.5.0 versions.	7.2	More Details
CVE-			

2026-96832	Shop manager PHP Object Injection in Content Egg <= 6.3.1 versions.	7.2	More Details
CVE-2026-96833	Editor PHP Object Injection in Ultimate Addons for Contact Form 7 <= 3.5.51 versions.	7.2	More Details
CVE-2026-102392	Shop manager PHP Object Injection in Extra Product Options For WooCommerce Custom Product Addons and Fields <= 3.3.8 versions.	7.2	More Details
CVE-2026-97245	Shop Worker Privilege Escalation in SureCart <= 4.7.2 versions.	7.2	More Details
CVE-2026-88396	ApiAdmin v5.0 and before is vulnerable to Directory Traversal. The admin file-upload endpoint POST /admin/Index/upload in ApiAdmin takes the uploaded file's extension verbatim there is no whitelist, blacklist or content check and move_uploaded_file() drops the file into the web-accessible directory public/upload/Ymd/. Any logged-in admin user can upload a .php file and reach it directly over HTTP, achieving remote code execution on the server.	7.2	More Details
CVE-2026-104890	Kunstmaan CMS is an open source content management system based on the Symfony framework. Prior to 7.3.2, src/Kunstmaan/MediaBundle/Helper/File/FileHandler.php performs the blacklisted_extensions check case-sensitively in FileHandler::getFilePath and lowercases the stored extension afterward. An authenticated backend user with media access can upload a mixed-case executable extension such as PHP that bypasses the check and is stored in the web-accessible media directory with an executable lowercase extension. The default blacklist also omits several server-executable extension types, allowing the same code-execution impact where the web server executes uploaded files. This issue is fixed in version 7.3.2.	7.2	More Details
CVE-2026-102099	Kiteworks Core before version 9.5.0 is vulnerable to Arbitrary File Write. An improper restriction of a user-supplied file path in a Kiteworks administrative export feature could allow an authenticated administrator to write a file to an arbitrary location on the underlying host, potentially leading to command execution on the appliance. Exploitation requires an existing, authenticated administrative account with access to the affected export function.	7.2	More Details
CVE-2026-93651	Author PHP Object Injection in Minimum and Maximum Quantity for WooCommerce <= 2.1.2 versions.	7.2	More Details
CVE-2026-102131	Kiteworks Email Protection Gateway rejected certain configuration settings, but its validation did not recognize every form in which they could be supplied. An authenticated administrator could potentially use an unrecognized form to have a file of their choosing written to the gateway and executed, resulting in code execution as the gateway service account.	7.2	More Details
CVE-2026-96649	The Frontend Post Submission Manager Lite – Frontend Posting WordPress Plugin plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via post_content Parameter (data-label DOM Sink) in all versions up to, and including, 1.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the site operator to have enabled guest post submission via the [fpsm] shortcode, which registers a publicly accessible AJAX handler gated only by a nonce emitted on every page containing the shortcode.	7.2	More Details
CVE-2026-103348	Deserialization of Untrusted Data vulnerability in Smackcoders Inc. WP Ultimate Exporter wp-ultimate-exporter allows Object Injection.This issue affects WP Ultimate Exporter: from n/a through 3.0.	7.2	More Details
CVE-2026-102142	A system notification template on the Kiteworks appliance was rendered by a template engine that evaluated expressions contained in the stored template body. An authenticated System Administrator could potentially store a crafted template that executed operating-system commands on the appliance when the notification was next sent.	7.2	More Details
CVE-2026-95263	Feehi CMS 2.1.1 is vulnerable to Incorrect Access Control. A low-privilege backend administrator with administrator-update permission can change the password of the built-in super administrator account. The server does not enforce protection for this account, and the update scenario does not require the old password.	7.2	More Details
CVE-2026-	Ghost is a Node.js content management system. From 6.10.3 until 6.64.0, a vulnerability in how Ghost loads theme translation files allowed an authenticated Administrator to execute arbitrary code on the	7.2	More Details

105677	server via a crafted theme. This issue is fixed in version 6.64.0.		
CVE-2026-102114	A command injection vulnerability in Kiteworks could allow a high-privileged authenticated administrator to execute arbitrary operating-system commands as root on the affected appliance node. Successful exploitation requires an administrative account with elevated privileges.	7.2	More Details
CVE-2026-102130	Kiteworks Email Protection Gateway did not sufficiently validate the content of an uploaded backup, and allowed an administrator to influence how the application loaded it. An authenticated administrator could potentially use this to execute arbitrary code on the gateway as the underlying service account.	7.2	More Details
CVE-2026-100506	Deserialization of Untrusted Data vulnerability in WP Spell Check WP Spell Check wp-spell-check allows Object Injection.This issue affects WP Spell Check: from n/a through 12.1.	7.2	More Details
CVE-2026-102129	A user-provisioning interface in Kiteworks Core did not verify that the requesting administrator was entitled to grant the role being assigned. An administrator whose delegated permissions covered role changes alone could therefore raise an account to full system-administrator privileges.	7.2	More Details
CVE-2026-102454	EasyFlow .NET developed by Digiwin has an Arbitrary File Upload vulnerability. Privileged remote attackers can upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2026-49878	In wpas_handle_robust_av_scs_rcv_action of robust_av.c, there is a possible out-of-bounds write due to a logic error in the code. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.	7.2	More Details
CVE-2026-102132	An administrative import function in Kiteworks Core did not verify that the requesting administrator was entitled to create the privileged integration credential being imported. A delegated administrator holding a single narrowly scoped administrative permission could therefore obtain full system administrator privileges, without any action by an existing system administrator.	7.2	More Details
CVE-2026-102119	A path traversal weakness in an optional, non-default administrative feature allowed an authenticated administrator to move files to unintended locations outside the feature's designated directory. This could potentially be leveraged to execute arbitrary code on the underlying system.	7.2	More Details
CVE-2026-102117	On deployments where the remote-support capability is licensed and enabled, an authenticated System Administrator who also possessed the key protecting the submitted data could redirect the underlying system's outbound support connection to a destination of their choosing. That destination could then have operating-system commands executed on the node and receive their output, potentially resulting in remote code execution with the privileges of a local service account.	7.2	More Details
CVE-2026-102116	-A weakness could have allowed an authenticated Kiteworks Email Protection Gateway administrator to write a file outside its intended location and cause the application to execute it, potentially resulting in remote code execution as the underlying service account.	7.2	More Details
CVE-2026-93617	Deserialization of Untrusted Data vulnerability in WP Sunshine Sunshine Photo Cart sunshine-photo-cart allows Object Injection.This issue affects Sunshine Photo Cart: from n/a through 3.7.1.	7.2	More Details
CVE-2026-97237	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.14.3 versions.	7.1	More Details
CVE-2026-104447	YesWiki before 4.6.7 contains a cross-site request forgery vulnerability in the autoupdate UpdateAction that allows attackers to delete installed packages via unprotected GET requests. Attackers can lure a logged-in administrator to a crafted link with action=delete and a package parameter to remove extensions like bazar, breaking core site functionality.	7.1	More Details
CVE-2026-97235	Unauthenticated Cross Site Scripting (XSS) in ThemeREX Addons < 2.45.0 versions.	7.1	More Details
CVE-2025-15643	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Fernandez Adsmonetizer adsensei-b30 allows Reflected XSS.This issue affects Adsmonetizer: from n/a through 3.2.4.	7.1	More Details
CVE-2026-97273	Unauthenticated Cross Site Scripting (XSS) in Premmerce Wishlist for WooCommerce <= 1.1.13 versions.	7.1	More Details

CVE-2026-86105	An improper authorization vulnerability in Fireware OS's Access Portal reverse proxy allows an authenticated, low-privileged Access Portal user to access other web applications they are not authorized for by sending a specially crafted request for a different resource which they are authorized to access.	7.1	More Details
CVE-2026-97065	Unauthenticated Cross Site Scripting (XSS) in Happyforms <= 1.26.15 versions.	7.1	More Details
CVE-2026-96836	Unauthenticated Cross Site Scripting (XSS) in Parsi Date <= 6.3 versions.	7.1	More Details
CVE-2026-97077	Unauthenticated Cross Site Scripting (XSS) in Ad Inserter <= 2.8.18 versions.	7.1	More Details
CVE-2026-97253	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kreatura LayerSlider allows Reflected XSS. This issue affects LayerSlider: from n/a through 8.4.0.	7.1	More Details
CVE-2026-97268	Unauthenticated Cross Site Scripting (XSS) in Premmerce Wishlist for WooCommerce <= 1.1.13 versions.	7.1	More Details
CVE-2026-97260	Unauthenticated Cross Site Scripting (XSS) in MaxGalleria <= 6.5.3 versions.	7.1	More Details
CVE-2026-97250	Unauthenticated Cross Site Scripting (XSS) in Geo Mashup <= 1.13.21 versions.	7.1	More Details
CVE-2026-104991	Phproject before 1.8.7 contains a missing object-level authorization vulnerability in the REST API issue endpoints (single_get, single_comments, single_comments_post) that allows authenticated API key holders to bypass the security.restrict_access confidentiality control by never invoking the allowAccess() authorization routine. Attackers can use a valid API key to read restricted issue contents and comments, including owner and author email addresses, and post unauthorized comments to issues they should not have access to.	7.1	More Details
CVE-2026-97271	Unauthenticated Cross Site Scripting (XSS) in WPFunnels <= 3.13.1 versions.	7.1	More Details
CVE-2026-97272	Unauthenticated Cross Site Scripting (XSS) in Premmerce Permalink Manager for WooCommerce <= 2.3.13 versions.	7.1	More Details
CVE-2026-102378	Unauthenticated Cross Site Scripting (XSS) in Parallax Section block <= 2.0.4 versions.	7.1	More Details
CVE-2026-97289	Unauthenticated Cross Site Scripting (XSS) in Quiz And Survey Master <= 11.2.6 versions.	7.1	More Details
CVE-2026-104478	Formwork before 2.3.13 contains a path traversal vulnerability in BackupController that allows authenticated panel users to read or delete arbitrary files. Attackers with backup download or delete permission can supply a base64-encoded backslash-separated traversal payload that bypasses PHP basename on Linux to access files outside the backup directory.	7.1	More Details
CVE-2026-104407	Cross-Site Request Forgery (CSRF) vulnerability in Blubrry Podcasting PowerPress Podcasting powerpress allows Cross Site Request Forgery.This issue affects PowerPress Podcasting: from n/a through 11.17.9.	7.1	More Details
CVE-2026-103266	Ghost versions 5.2.0 through versions prior to 6.62.0 allow a remote attacker, without authentication, to abuse the Stripe Checkout flow to attach a paid subscription to an existing member, modify that member's name, and inject content into newsletters sent to the member. Depending on the recipient's email client, the injected content may be rendered, resulting in HTML injection or cross-site scripting (XSS).	7.1	More Details

CVE-2026-103256	n8n versions before 2.39.6 and 2.40.0 before 2.40.1 contain a credentials leak vulnerability in the Wekan and Baserow username-and-password credentials that sends unencrypted passwords to unvalidated hosts. Attackers with credential update permissions can modify the host field to receive account passwords at arbitrary hosts, bypassing domain validation controls.	7.1	More Details
CVE-2026-103251	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a validation bypass vulnerability in the community package installation handler for queue mode deployments. Attackers with Redis write access can bypass name validation, permission checks, checksum verification, and npm safety checks to install arbitrary npm packages across all cluster instances without authentication.	7.1	More Details
CVE-2026-96577	A flaw was found in oc-mirror. During mirroring operations, the embedded local cache registry binds to all network interfaces without authentication or encryption instead of restricting access to the local system. An unauthenticated attacker on an adjacent network can connect to the exposed service to push tampered container images, delete cached images, or access mirrored content.	7.1	More Details
CVE-2026-103054	AiSOC versions before 12.0.0 contain an authorization bypass vulnerability in the MSSP module that allows authenticated users to add arbitrary tenants to portfolios they own. Attackers can submit tenant UUIDs via the add_tenants_to_portfolio endpoint to claim unclaimed tenants and read their security alerts, incidents, and posture metrics without consent.	7.1	More Details
CVE-2026-96352	Unauthenticated Cross Site Scripting (XSS) in YITH WooCommerce Ajax Search <= 2.28.0 versions.	7.1	More Details
CVE-2026-96830	Unauthenticated Cross Site Scripting (XSS) in GiveWP <= 4.16.9 versions.	7.1	More Details
CVE-2026-93512	Unauthenticated Cross Site Scripting (XSS) in JW Player for WordPress <= 2.3.11 versions.	7.1	More Details
CVE-2026-104444	YesWiki before 4.6.7 contains an authorization bypass vulnerability in the comments API editComment route that allows authenticated low-privilege users to overwrite arbitrary pages or comments by supplying their own page as the pagetag field. Attackers can send a POST request to the api/comments endpoint targeting a victim tag, bypassing per-page write ACLs to replace content and reparent existing pages or comments.	7.1	More Details
CVE-2026-103242	A heap-based buffer overflow flaw was found in rpm. RPMTAG_FILESIGNATURES in a crafted, unsigned RPM package's main header is declared with the wrong header type, causing hex2binv() to allocate a one-byte buffer and then write the tag's attacker-controlled, hex-decoded content — of attacker-chosen length — past the end of that allocation. This is reachable via rpm2cpio, rpm2archive, and rpm -qlvp on an untrusted package.	7.1	More Details
CVE-2026-100507	Unauthenticated Cross Site Scripting (XSS) in If-So Dynamic Content Personalization <= 1.10.1 versions.	7.1	More Details
CVE-2026-100515	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Photo Reviews for WooCommerce woo-photo-reviews allows Reflected XSS.This issue affects Photo Reviews for WooCommerce: from n/a through 1.2.30.	7.1	More Details
CVE-2026-85215	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in GG Soft Software Services Inc. Paperwork allows SQL Injection. This issue affects Paperwork: through 2026-09-09.	7.1	More Details
CVE-2026-102385	Unauthenticated Cross Site Scripting (XSS) in Ninja Forms <= 3.15.3 versions.	7.1	More Details
CVE-2026-102395	Unauthenticated Cross Site Scripting (XSS) in Easy Google Maps <= 1.14.6 versions.	7.1	More Details
CVE-2026-102396	Unauthenticated Cross Site Scripting (XSS) in Ultimate Maps by Supsysitic <= 1.5.5 versions.	7.1	More Details
CVE-			More

2026-102398	Unauthenticated Cross Site Scripting (XSS) in Popup by Supsysitic <= 1.13.1 versions.	7.1	Details
CVE-2026-105633	Plane is an open-source project management tool. Prior to 1.4.0, the V2 issue-attachment PATCH endpoint accepts issue_id in the URL but omits it from the database query. A project member can use an issue_id they control in the URL while targeting another user's attachment by its pk UUID. Because the server matches only pk, workspace, and project_id, it modifies the attachment regardless of the issue_id in the URL. When the attachment is pending and has not been confirmed as uploaded, the PATCH handler sets created_by = request.user and transfers attachment ownership to the attacker. This issue is fixed in 1.4.0.	7.1	More Details
CVE-2026-27371	Unauthenticated Cross Site Scripting (XSS) in WPFunnels <= 3.13.1 versions.	7.1	More Details
CVE-2026-105629	Plane is an open-source project management tool. Prior to 1.4.0, BulkEstimatePointEndpoint.destroy resolves an estimate point through a bare primary-key lookup without workspace, project, or estimate scoping. An administrator or member of one workspace can permanently delete an estimate point belonging to another workspace by supplying the target UUID in a URL under the attacker's own workspace. This creates a destructive cross-tenant IDOR. This issue is fixed in 1.4.0.	7.1	More Details
CVE-2026-93514	Unauthenticated Cross Site Scripting (XSS) in Notification for Telegram <= 3.5.2 versions.	7.1	More Details
CVE-2026-96820	Subscriber Cross Site Scripting (XSS) in Awesome Support <= 6.3.9 versions.	7.1	More Details
CVE-2026-103488	In JetBrains YouTrack before 2026.2.19422 missing authorisation allowed authenticated users to add themselves to project teams and access restricted issues	7.1	More Details
CVE-2026-93770	Unauthenticated Cross Site Scripting (XSS) in WP Statistics <= 14.16.13 versions.	7.1	More Details
CVE-2026-94078	Unauthenticated Cross Site Scripting (XSS) in Site Reviews <= 8.3.1 versions.	7.1	More Details
CVE-2026-94081	Unauthenticated Cross Site Scripting (XSS) in WordPress Persistent Login <= 3.1.3 versions.	7.1	More Details
CVE-2026-94499	Subscriber Broken Access Control in FormGent <= 1.12.2 versions.	7.1	More Details
CVE-2026-104975	Plane is an open-source project management tool. Prior to 1.4.0, Plane's dashboard asset endpoints in plane/app/views/asset/v2.py were remediated for two cross-tenant asset IDORs, CVE-2026-27705 and CVE-2026-46558. Those fixes added a membership check and project_id and workspace__slug scoping to the asset endpoints in that file. The Spaces app in plane/space/views/asset.py serves related public-board operations under /api/public/ but was not remediated. Its EntityAssetEndpoint and AssetRestoreEndpoint resolve a DeployBoard from a public anchor and then read or modify FileAsset rows scoped only to the board's workspace, without a membership check or project_id constraint. An attacker can therefore read, overwrite, or restore assets across projects and workspaces. This issue is fixed in 1.4.0.	7.1	More Details
CVE-2026-91832	The WP Mobile Menu WordPress plugin before 2.9 does not correctly verify the nonce on its settings import, so an attacker can import arbitrary WP Mobile Menu WordPress plugin before 2.9 settings through a cross-site request in an administrator's session, and the imported values are then output unescaped to every visitor, resulting in Stored Cross-Site Scripting.	7.1	More Details
CVE-2026-88797	The Vayu X WordPress theme before 1.0.6 does not perform any capability check on one of its AJAX actions and exposes the nonce guarding it to every logged-in user, allowing any authenticated user, such as a subscriber, to install and activate any hosted on the WordPress.org repository.	7.1	More Details
CVE-2026-	Unauthenticated Cross Site Scripting (XSS) in Classified Listing <= 6.1.3 versions.	7.1	More

96351			Details
CVE-2026-96814	Unauthenticated Cross Site Scripting (XSS) in WooCommerce Product Table Lite <= 5.6.7 versions.	7.1	More Details
CVE-2026-96816	Unauthenticated Cross Site Scripting (XSS) in Trusted Shops Easy Integration for WooCommerce <= 2.0.6 versions.	7.1	More Details
CVE-2026-96819	Subscriber Cross Site Scripting (XSS) in oik <= 4.15.4 versions.	7.1	More Details
CVE-2026-47554	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where improper verification of cryptographic signatures may cause signature verification to be bypassed under memory pressure. A successful exploit of this vulnerability might lead to denial of service and data tampering.	7.1	More Details
CVE-2026-102282	adm-zip is a JavaScript library for creating and extracting ZIP archives in Node.js. Prior to 0.6.1, adm-zip applies the Unix permission bits stored in a zip entry directly to the extracted file via <code>`fs.chmodSync()`</code> when <code>`keepOriginalPermission=true`</code> is passed to <code>`extractAllTo()`</code> / <code>`extractEntryTo()`</code> — and it never filters the <code>setuid/setgid/sticky</code> bits out of those bits. A zip crafted by an attacker can therefore produce an extracted binary with mode <code>`04755`</code> . When extraction runs as root (the default posture in Docker builds, CI runners, and privileged install steps — the exact environments where this flag is used), the resulting root-owned <code>setuid</code> file is executed later by a lesser-privileged user, turning the attacker's code into a root execution. Version 0.6.1 fixes the issue.	7.1	More Details
CVE-2026-105741	Langflow is a tool for building and deploying AI-powered agents and workflows. From 1.5.0 until 1.10.3, an IP spoofing vulnerability in the Model Context Protocol (MCP) configuration installation endpoint (POST /api/v1/mcp/project/{project_id}/install) allowed authenticated remote attackers to bypass the "local-only" access restriction. By sending a spoofed X-Forwarded-For: 127.0.0.1 header, an attacker could make the server treat the request as originating from localhost, letting them write/overwrite an MCP client configuration file on the server's filesystem. This vulnerability is fixed in 1.10.3.	7.1	More Details
CVE-2026-100510	Unauthenticated Cross Site Scripting (XSS) in Post and Page Builder by BoldGrid <= 1.27.14 versions.	7.1	More Details
CVE-2026-47602	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode driver where a local user can cause the driver to dereference an untrusted pointer. A successful exploit of this vulnerability might lead to denial of service and information disclosure.	7.1	More Details
CVE-2026-102391	Unauthenticated Cross Site Scripting (XSS) in JetFormBuilder <= 3.6.5.4 versions.	7.1	More Details
CVE-2026-103342	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Reflected XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.20.	7.1	More Details
CVE-2026-92412	The Five Star Restaurant Reviews WordPress plugin before 2.3.14 does not properly escape a user-supplied value before outputting it into an HTML tag, allowing unauthenticated attackers to inject arbitrary web script that runs in the browser of anyone tricked into submitting a crafted request, including a logged-in administrator.	7.1	More Details
CVE-2026-94171	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme CURCY woo-multi-currency allows DOM-Based XSS.This issue affects CURCY: 2.2.18.	7.1	More Details
CVE-2026-97290	Unauthenticated Cross Site Scripting (XSS) in Photonic Gallery & Lightbox for Flickr, SmugMug & Others <= 3.36 versions.	7.1	More Details
CVE-2026-103062	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs TranslatePress translatepress-multilingual allows Stored XSS.This issue affects TranslatePress: from n/a through 3.3.6.	7.1	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-		More

2026-103344	elements-for-elementor allows Reflected XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.20.	7.1	Details
CVE-2026-103354	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP Gutenberg Blocks by Kadence Blocks kadence-blocks allows Stored XSS.This issue affects Gutenberg Blocks by Kadence Blocks: from n/a through 3.7.11.1.	7.1	More Details
CVE-2026-97276	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP Statistics wp-statistics allows Reflected XSS.This issue affects WP Statistics: from n/a through 14.16.14.	7.1	More Details
CVE-2026-102109	A SQL injection vulnerability existed in Kiteworks Secure Data Forms, where a value derived from the authenticated user's stored account data was incorporated into a database query without proper sanitization. An authenticated user could potentially influence that value to inject SQL. Exploitation requires an authenticated session and applies only to deployments where a specific optional feature is in use.	7.1	More Details
CVE-2026-102376	Subscriber Cross Site Scripting (XSS) in Branda <= 3.4.32 versions.	7.1	More Details
CVE-2026-104463	YesWiki before 4.6.7 contains a server-side request forgery vulnerability that allows unauthenticated attackers to trigger server requests by sending signed Follow activities to the public forms actor inbox route. Attackers sign requests with their own keyld while supplying internal actor URLs in the body, reaching internal hosts or cloud metadata via blind GET and POST requests.	7.0	More Details
CVE-2026-47596	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user can write to read-only memory because the memory's permissions are not preserved. A successful exploit of this vulnerability might lead to code execution and escalation of privileges.	7.0	More Details
CVE-2026-102127	An XML parser used by Kiteworks Email Protection Gateway did not restrict external entity references. Where an optional, non-default message-processing feature is enabled, a remote and unauthenticated sender could potentially use a crafted message to read files accessible to the gateway service account, including cryptographic key material and credentials, and have them sent to a destination they control.	7.0	More Details
CVE-2026-58880	In handle_app_val_response of btif_rc.cc, there is a possible way to achieve code execution due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2026-47598	NVIDIA GPU Display Driver for Linux contains a vulnerability in the open-source kernel module event delivery path where an unprivileged local user could cause a use-after-free through a race between asynchronous event delivery and file close. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	7.0	More Details
CVE-2026-47582	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.0	More Details
CVE-2026-100275	In JetBrains YouTrack before 2026.2.19197 stored XSS in the workflow error notification toast was possible	6.9	More Details
CVE-2026-94239	The Loco Translate WordPress plugin before 2.8.9 does not sanitise and escape some bundle configuration values before outputting them back in an admin page, allowing users with the translator capability and above to perform Stored Cross-Site Scripting attacks against high privilege users such as administrators.	6.8	More Details
CVE-2026-105119	OpenAM before 16.1.3 applies its OAuth2 Provider PKCE enforcement only to authorization requests whose response_type is exactly code, so codes issued through OpenID Connect hybrid flows (code token, code id_token, code token id_token) carry no bound challenge. An attacker who intercepts such a code can redeem it for a public client's tokens with any non-empty code_verifier.	6.8	More Details
CVE-2026-103279	Ghost versions from 3.10.0 before 6.34.0 fail to fully invalidate all sessions after a password change. Attackers with a stolen session cookie can maintain access to user accounts even after the associated user changes their password.	6.8	More Details
CVE-2026-103293	The MPG WordPress plugin before 4.2.3 does not validate that the dataset source supplied when importing a project is a remote URL before treating it as a local filesystem path and copying that file into a publicly accessible uploads folder. This makes it possible for users with the Editor role and above to read the contents of arbitrary files on the server, with the copied file then retrievable by	6.8	More Details

	unauthenticated visitors.		
CVE-2026-20544	In meta, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11049530 / ALPS11480843; Issue ID: MSV-7935.	6.8	More Details
CVE-2026-104964	Plane is an open-source project management tool. Prior to 1.4.0, Plane's project update endpoint authorizes the caller against the workspace slug in the request URL but loads the target project globally by UUID without binding it to that workspace. An administrator of one workspace can modify a project in another workspace when the victim project UUID is known. This violates tenant isolation and permits unauthorized cross-workspace changes to project metadata and configuration. This issue is fixed in 1.4.0.	6.8	More Details
CVE-2026-97242	Author Arbitrary File Deletion in WEBO MCP <= 3.0.18 versions.	6.8	More Details
CVE-2026-85001	The EmbedPress WordPress plugin before 4.6.7 does not sanitise and escape one of its Elementor widget settings before outputting it into an HTML attribute, which could allow users with the Contributor role or above to inject arbitrary web scripts that execute when the affected content is viewed.	6.8	More Details
CVE-2026-85415	The Audio Player Block WordPress plugin before 1.6.3 does not validate the scheme of a user-supplied URL before using it as a link target, allowing users with the Contributor role and above to store malicious JavaScript that executes in the session of any user who later triggers the link (such as an administrator or editor reviewing the post).	6.8	More Details
CVE-2026-91022	The Motors WordPress plugin before 1.4.124 does not sanitise and escape a listing badge setting before outputting it inside an HTML attribute, allowing users with a custom, administrator-assigned listing-management role to inject arbitrary web scripts that execute when a listing is viewed by any visitor, including an administrator.	6.8	More Details
CVE-2026-96824	Editor Arbitrary File Deletion in Template Kit - Import <= 1.0.16 versions.	6.8	More Details
CVE-2026-88782	The Kubio AI Page Builder WordPress plugin before 2.9.3 does not validate the URI scheme of a user-supplied value before outputting it as a link target, allowing users with the contributor role and above to store a payload which executes in the browser of anyone who follows the link, including an administrator previewing the unpublished submission.	6.8	More Details
CVE-2026-94238	The Loco Translate WordPress plugin before 2.8.9 does not restrict which file paths its translation file routes will read, allowing users granted the Loco Translate WordPress plugin before 2.8.9's translator capability to retrieve the contents of files of certain types from anywhere on the server, including outside the web root.	6.8	More Details
CVE-2026-85016	The Unlimited Elements for Elementor WordPress plugin before 2.0.21 does not escape an icon value before concatenating it into an HTML attribute in its shared widget-parameter processor, allowing users with Contributor access (who do not hold unfiltered_html) to store a payload that executes when the page is rendered.	6.8	More Details
CVE-2026-87777	The Hostinger Reach WordPress plugin before 1.8.3 does not sanitize and escape a widget setting before outputting it in the editor preview, allowing users with contributor-level access and above to inject arbitrary web scripts that will execute in the session of a higher-privileged user who opens the affected content in the editor.	6.8	More Details
CVE-2026-13718	The Tabs Responsive WordPress plugin through 2.5 does not sanitize the content of WooCommerce product tabs before storing and rendering it, allowing a shop manager to store JavaScript that executes when any user, including an administrator, views the product page.	6.8	More Details
CVE-2026-17005	The Horizontal scrolling announcements WordPress plugin through 2.6 does not sanitise and escape one of its announcement settings before outputting it into an attribute context on the front end, allowing users granted access to the announcement management page (Contributor and above, once permitted) to perform Stored Cross-Site Scripting attacks that execute in the browser of anyone viewing the announcement.	6.8	More Details
CVE-2026-92424	The Content Egg WordPress plugin before 11.9.0 does not verify that a user running its bulk content-import feature is authorized for the import preset they select, and switches to the preset author's identity before creating the resulting post, allowing users with contributor-level access and above to store arbitrary web scripts unfiltered under a privileged user's account, executing in the context of	6.8	More Details

	anyone who later views that content.		
CVE-2026-104469	YesWiki before 4.6.7 contains a session fixation vulnerability that allows attackers to hijack authenticated sessions because login does not regenerate the PHP session ID. Attackers who set or learn a victim's pre-authentication YesWiki-* session cookie can reuse it after login to access private content and perform actions with the victim's privileges.	6.8	More Details
CVE-2026-105644	Ghost is a Node.js content management system. From 4.0.0 until 6.67.0, SVG images included in content imports were stored without sanitization. An attacker who convinced an Administrator to import a crafted file could host scripts on the site's domain, possibly resulting in compromise of staff users' admin sessions. This issue is fixed in version 6.67.0.	6.8	More Details
CVE-2026-85568	The Unlimited Elements for Elementor WordPress plugin before 2.0.21 does not correctly handle a search value before rewriting an already prepared SQL statement, allowing unauthenticated users to perform SQL injection attacks and to retrieve non-public content, when a related widget option is set away from its default.	6.8	More Details
CVE-2025-71427	Office-PowerPoint-MCP-Server through 2.0.7 contains a path traversal vulnerability that allows MCP callers to write and read files outside the working directory by supplying absolute paths or ../ sequences. Attackers can steer an AI agent via prompt injection to abuse save_presentation, open_presentation, or manage_image output_path to overwrite any server-writable file or load external files.	6.8	More Details
CVE-2026-78862	An issue in Mercusys AC12 V2 allows a local attacker to execute arbitrary code via the UART serial interface on the printed circuit board (PCB)	6.8	More Details
CVE-2026-103258	n8n versions before 2.39.6 and 2.40.0 before 2.40.1 contain an unescaped parameter interpolation vulnerability in SendGrid, Freshservice, and ServiceNow nodes that allows attackers to bypass filters by breaking out of query literals. Attackers can exploit this by binding vulnerable node parameters to untrusted external input to widen single-record lookups into match-all queries, exposing bulk data including contact lists, tickets, and directory entries.	6.8	More Details
CVE-2026-102141	Two Kiteworks Core cluster-management operations did not validate file paths supplied to them, so an attacker holding root on one node of a cluster could write files as root onto another node and cause them to be executed there. Exploitation requires backend root access on a cluster node and a pending software patch present on the target node.	6.7	More Details
CVE-2026-47543	VIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause improper input validation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47515	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an out-of-bounds read via an unbounded string operation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-78229	Image Scanner Driver for Linux contains an OS command injection vulnerability. An attacker who can log in to a Linux system where the affected product is installed may execute an arbitrary OS command by making certain preparations.	6.7	More Details
CVE-2026-20588	In mtee, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11383899; Issue ID: MSV-9607.	6.7	More Details
CVE-2026-20587	In mtee, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11383899; Issue ID: MSV-9608.	6.7	More Details
CVE-2026-20579	In vdec, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11383899; Issue ID: MSV-9800.	6.7	More Details
CVE-2026-12545	A flaw was found in rubygem-hammer_cli. A command injection vulnerability exists in Hammer CLI and the Railties (Ruby on Rails) component distributed with Satellite due to the insecure interpolation of the \$EDITOR environment variable into the Ruby system() method. By passing a single interpolated string to system(), the application invokes a system shell (/bin/sh) that interprets shell metacharacters (e.g., ;, , &).	6.7	More Details

CVE-2026-47527	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the firmware where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-20542	In apusys, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11076799; Issue ID: MSV-8143.	6.7	More Details
CVE-2026-47542	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause improper input validation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47547	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the firmware where an attacker could cause improper input validation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47539	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an incorrect numeric conversion. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47544	NVIDIA vGPU Virtual GPU Manager for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-20528	In ccci, there is a possible out of bounds write and read due to a missing bounds check. This could lead to local information disclosure, memory corruption, crashes, or privilege escalation if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS11428950 (Note: For MT6880, MT6890) / ALPS10563453 (Note: For MT6980D, MT6990, MT6986, MT6986D, MT6813, MT6988) / AUTO00858766 (Note: For MT2735, MT2737); Issue ID: MSV-9893.	6.7	More Details
CVE-2026-20529	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11276677; Issue ID: MSV-9217.	6.7	More Details
CVE-2026-20530	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11292777; Issue ID: MSV-9195.	6.7	More Details
CVE-2026-47538	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the firmware where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-20533	In display, there is a possible escalation of privilege due to an integer overflow. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11296678; Issue ID: MSV-9167.	6.7	More Details
CVE-2026-20535	In aidl, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11185216; Issue ID: MSV-9039.	6.7	More Details
CVE-2026-20536	In aidl, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11242428; Issue ID: MSV-9038.	6.7	More Details
CVE-2026-47537	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47529	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47532	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-	In aidl, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed	6.7	More

20537	for exploitation. Patch ID: ALPS11185225; Issue ID: MSV-9024.		Details
CVE-2026-47533	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an improper validation of an array index. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-105688	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, create-team-invitations and the invitation acceptance path allow a non-owner team administrator to assign the owner role because invitation roles are persisted and applied without the role-ceiling check used by update-team-member-role. An administrator can invite another account as an owner, create multiple owners, and then use the new owner account to obtain owner-only control over the team. This issue is fixed in version 2.18.0.	6.7	More Details
CVE-2026-104474	OpenLiteSpeed before 1.9.3 contains a local privilege escalation vulnerability in admin/misc/lsup.sh that runs unverified update packages from a nobody-writable directory as root. Attackers controlling the nobody web process can replace the package in /usr/local/lsws/autoupdate/ before extraction, so its install.sh runs as root on the next update.	6.7	More Details
CVE-2026-20589	In venc, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS11383899; Issue ID: MSV-9606.	6.7	More Details
CVE-2026-47546	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the firmware where an attacker could cause improper input validation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47522	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause improper input validation. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47509	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47524	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-47525	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause an improper validation of an array index. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.7	More Details
CVE-2026-77804	In Progress® Telerik® Fiddler® Classic for Windows, versions prior to v6.0.20262.10021, a time-of-check time-of-use (TOCTOU) race condition exists in the installation of the HTTPS interception root certificate into the Local Computer certificate store. Fiddler writes the certificate to a temporary file in a user-writable location and then launches the external TrustCert helper application, which elevates and imports the certificate from that file. A local threat actor with low privileges who replaces the temporary file between the time it is written and the time the elevated helper reads it can cause an attacker-supplied root certificate to be installed in the Local Computer Trusted Root Certification Authorities store, enabling subsequent interception and modification of TLS-protected traffic on the machine. Successful exploitation requires the user to initiate the certificate trust operation and approve the elevation prompt.	6.6	More Details
CVE-2026-103494	In JetBrains YouTrack before 2026.2.19422 privilege escalation was possible via user group membership changes	6.6	More Details
CVE-2026-102135	On a Kiteworks Email Protection Gateway cluster with database replication enabled, a party trusted by the cluster could submit a crafted serialized object that was deserialized without sufficient validation, potentially allowing code execution as the gateway service account. Replication is disabled by default, and exploitation requires control of a trusted cluster peer or administrative access to the appliance.	6.6	More Details
CVE-2026-102145	An authenticated administrator could cause the server to issue requests to, and interact with, internal network services that are not meant to be reachable through this interface. On its own this did not result in code execution.	6.6	More Details
CVE-	Image Scanner Driver for Linux contains a link following vulnerability. An attacker who can log in to a		

2026-81310	Linux system where the product is installed may overwrite arbitrary files by using a special method in advance.	6.6	More Details
CVE-2026-91051	The EWWW Image Optimizer WordPress plugin before 8.8.0 does not prevent authenticated users with author-level permissions from storing a serialized value in a post meta field that is deserialized when the post is rendered, allowing them to perform PHP Object Injection, which can lead to remote code execution when a suitable gadget chain is present via another installed EWWW Image Optimizer WordPress plugin before 8.8.0 or .	6.6	More Details
CVE-2026-85015	The Unlimited Elements for Elementor WordPress plugin before 2.0.21 does not sanitise file paths inside uploaded archives before extracting them, allowing authenticated users with access to its asset-management feature (Administrators by default, or Editors when a non-default Unlimited Elements for Elementor WordPress plugin before 2.0.21 setting is enabled) to write arbitrary files, including executable PHP, outside the intended upload directory on servers where the PHP zip extension is unavailable, leading to Remote Code Execution.	6.6	More Details
CVE-2026-102133	An optional, separately licensed repository-connector feature in Kiteworks Core did not neutralize special characters in a user-supplied path before passing it to an external command. An authenticated system administrator could inject additional commands and write arbitrary content to files owned by the service account running the connector, enabling code execution in that account's context; exploitation additionally requires network egress from the appliance to a system under the attacker's control.	6.6	More Details
CVE-2026-97265	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock. Jetimpex Inc. JetEngine allows Stored XSS. This issue affects JetEngine: from n/a through 3.8.15.3.	6.5	More Details
CVE-2026-94077	Contributor Cross Site Scripting (XSS) in Safe SVG <= 2.5.0 versions.	6.5	More Details
CVE-2026-67075	HCL Digital Experience is affected by improper input sanitation. This can result in HTML injection which could be leveraged in content spoofing from a trusted domain. Apply HCL Digital Experience 9.5 CF238 or later to address this.	6.5	More Details
CVE-2026-94074	Unauthenticated Broken Access Control in Simply Schedule Appointments <= 1.6.12.29 versions.	6.5	More Details
CVE-2026-51892	infiniflow ragflow 0.24.0 is vulnerable to Incorrect Access Control via /v1/document/get/<doc_id>.	6.5	More Details
CVE-2026-103884	A flaw was found in the X.509 client certificate authenticator of Keycloak. When CRL Distribution Point checking is enabled, the server fails to properly validate the file paths provided in a client certificate. An attacker can provide a specially crafted certificate that causes the server to attempt to read sensitive files from the local system or exhaust memory by loading extremely large files, potentially leading to information disclosure or a system crash.	6.5	More Details
CVE-2026-51894	infiniflow ragflow 0.24.0 is vulnerable to Incorrect Access Control via run_mindmap. A reachable path accepts a caller-selected object or tenant identifier and reaches a data-access operation without a visible owner, tenant, workspace, or membership binding on that object.	6.5	More Details
CVE-2026-102457	EasyFlow .NET developed by Digiwin has an Arbitrary File Read vulnerability. Authenticated remote attackers can exploit this vulnerability to download arbitrary system files.	6.5	More Details
CVE-2026-105129	LaraDashboard before 1.4.8 contains an incorrect authorization vulnerability that allows authenticated users with only settings.view permission to read stored secrets through the settings API. Attackers can query GET /api/settings or /api/settings/{option_name} to retrieve plaintext AI provider API keys, mail credentials, passwords and tokens.	6.5	More Details
CVE-2026-102124	A Kiteworks appliance setup interface did not enforce authentication once the appliance had completed initial configuration. An unauthenticated attacker with network access to the appliance could read and modify a limited set of setup records, including a contact name and email address captured during initial configuration.	6.5	More Details
CVE-2026-103627	Information leak in SVG in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to obtain sensitive information via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE-2026-103592	simple-php-router through 5.4.1.7 contains an IP restriction bypass vulnerability in the IpRestrictAccess middleware that allows remote unauthenticated attackers to bypass IP whitelist and blacklist protections. Attackers can spoof X-Forwarded-For, CF-Connecting-IP, or Client-IP headers to impersonate whitelisted addresses or evade blacklists, gaining access to IP-restricted routes.	6.5	More Details
CVE-2026-94674	Contributor Cross Site Scripting (XSS) in Pixel Manager for WooCommerce <= 1.69.0 versions.	6.5	More Details
CVE-2026-94029	Server-side memory exhaustion in Apache MINA SSHD 1.0.0 to 2.19.0 and 3.0.0-M1 to 3.0.0-M5, component sshd-sftp, in the SFTP v6 check-file-name/check-file-handle extension. Apache MINA SSHD is a Java library for client-side and server-side SSH. Using a very small "block size" (for instance 256, which is the minimum) on a huge file generates many (file size / block size) hashes. The resulting SFTP reply message was accumulated fully in memory server-side, which could, with a suitably large (possibly sparse) file exhaust the server-side memory, taking down the server. Users are recommended to upgrade to version 2.20.0 or 3.0.0-M6, which fix this issue by imposing a maximum limit on the size of the reply. Many SFTP implementations have a general limit on the size of SFTP messages anyway; typically 256kB as in OpenSSH or also in Apache MINA SSHD.	6.5	More Details
CVE-2026-96338	Subscriber Cross Site Scripting (XSS) in Profile Builder <= 4.0.2 versions.	6.5	More Details
CVE-2026-90974	The WP Fusion Lite WordPress plugin before 3.48.0 does not require authentication on a settings handler that runs during admin initialization, allowing unauthenticated users to overwrite the site's CRM integration endpoint and credentials, after which synced user data is delivered to an attacker-chosen host.	6.5	More Details
CVE-2026-96834	Subscriber Sensitive Data Exposure in GiveWP <= 4.16.9 versions.	6.5	More Details
CVE-2026-102397	Unauthenticated Broken Access Control in Ultimate Maps by Supsysitic <= 1.5.5 versions.	6.5	More Details
CVE-2026-96829	Contributor Cross Site Scripting (XSS) in The Plus Addons for Elementor Page Builder Lite <= 6.5.1 versions.	6.5	More Details
CVE-2026-55265	In multiple functions of PduParser.java, there is a possible out of bounds read due to a missing bounds check. This could lead to a remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	6.5	More Details
CVE-2026-100157	The The WP Ultimate Review plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.4.3. 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. The nonce required to pass the only gate is emitted to unauthenticated visitors via the public review form, and submitted shortcode payloads are auto-published without admin approval by default, meaning exploitation requires no account and no privileged interaction.	6.5	More Details
CVE-2026-96613	The Meari IoT Cloud Platform OpenAPI Service is vulnerable to an authorization flaw that allows authenticated users to access the complete device shadow of any device by specifying its device ID. This vulnerability exposes sensitive information, such as device credentials, owner details, network data, and telemetry, without verifying any relationship between the requester and the target device.	6.5	More Details
CVE-2026-104434	ZcashFoundation Zebra zebra-rpc before 8.0.0 and zebrad before 4.5.0 contain a reachable assertion in the z_listunifiedreceivers RPC handler, which calls expect() on Sapling receiver parsing that fails for Unified Addresses carrying invalid Jubjub points. Authenticated RPC clients can submit such an address to abort the zebrad process, repeatably keeping the node offline.	6.5	More Details
CVE-2026-51895	Ragflow 0.24.0 and prior contains improper access control in update_metadata_setting (api/apps/kb_app.py). Depending on the exposed entry, an attacker can perform unauthorized cross-session or privilege-crossing operations.	6.5	More Details
CVE-2026-103491	In JetBrains YouTrack before 2026.2.19422 iDOR in the issue activities API allowed reading restricted issues	6.5	More Details

CVE-2026-94483	Next.js is a React framework for building full-stack web applications. From 16.0.0 until 16.3.8, Image Optimization can follow attacker-controlled DNS resolution for a remote URL that matches images.remotePatterns, allowing the optimized image fetch to reach private IP addresses after the URL passes the allow-list check. Applications without images.remotePatterns are not affected. Administrators unable to upgrade should audit allow-listed hosts and avoid entries whose DNS records are not trusted. This issue is fixed in version 16.3.8.	6.5	More Details
CVE-2026-102456	EasyFlow .NET developed by Digiwin has an SQL Injection vulnerability. Authenticated remote attackers can inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2026-51896	infiniflow ragflow 0.25.3 contains improper access control in resume (api/apps/connector_app.py). Depending on the exposed entry, an attacker can perform unauthorized cross-session or privilege-crossing operations.	6.5	More Details
CVE-2026-56097	A flaw was found in rubygem-katello. An SQL injection vulnerability exists in the Red Hat Satellite Katello Registry Proxy. The application fails to sanitize input parameters used in database queries within the RegistryProxiesController. The methods check_blob_push_org_label and get_matching_products_from_org take user-supplied labels directly from the request path and interpolate them into raw SQL fragments. This flaw is accessible to a user with only the create_personal_access_tokens permission, even if the user access is restricted, with no Organization or Location assigned.	6.5	More Details
CVE-2026-96347	Subscriber Insecure Direct Object References (IDOR) in Bookly <= 28.2 versions.	6.5	More Details
CVE-2026-102588	A flaw was found in Moodle. The XML grade import feature lacks proper Cross-Site Request Forgery (CSRF) token validation. By tricking an authenticated user with grade management permissions into visiting a malicious webpage, an attacker can trigger unauthorized requests on the victim's behalf. This flaw allows a remote attacker to set or overwrite student grades without authorization.	6.5	More Details
CVE-2026-101879	OpenClaw Windows Node before 2026.7.1-3 contains a missing authorization vulnerability in NodeService capture handlers that allows connected gateways or agents to perform screen snapshots, camera snaps, and location captures without consent prompts. Attackers can invoke screen.snapshot, camera.snap, and location.get over the node WebSocket to silently capture screenshots, photograph users through webcams, and obtain device geolocation without user interaction.	6.5	More Details
CVE-2026-104446	YesWiki before 4.6.7 contains an authentication bypass in the contact mail AJAX handler that allows unauthenticated attackers to send email through the wiki's SMTP server. Attackers can POST an XMLHttpRequest to the mail handler without field or type parameters, supplying arbitrary recipient, sender, subject and body for spam and phishing.	6.5	More Details
CVE-2026-103001	PyJWT is a Python implementation of JSON Web Token standards. From 2.11.0 through 2.13.0, PyJWT's PyJWT._merge_options() method can modify a caller-supplied mutable options mapping when verify_signature is false. If an application reuses that same mapping for a later decode() or decode_complete() call and changes verify_signature to true, the mapping can retain false values for expiration, not-before, issued-at, audience, issuer, subject, and JWT ID checks. A signed token with invalid registered claims can then be accepted without disabling signature verification, but applications that create a fresh options mapping for each call are not affected.	6.5	More Details
CVE-2026-102666	The Joyland AI app contains hard-coded credentials for the GeTui push notification service, allowing an attacker to access the GeTui REST API and send push notifications containing arbitrary content to any user, group of users, or all users of the app at once.	6.5	More Details
CVE-2026-102386	Subscriber Cross Site Scripting (XSS) in WP Photo Album Plus <= 9.3.02.003 versions.	6.5	More Details
CVE-2026-97304	Missing Authorization vulnerability in Arraytics Timetics timetics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Timetics: from n/a through 1.0.63.	6.5	More Details
CVE-2026-100509	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webful Creations RepairBuddy computer-repair-shop allows Stored XSS.This issue affects RepairBuddy: from n/a through 4.1225.	6.5	More Details
CVE-2026-85209	Missing Authorization vulnerability in AVEZ Electronics Communication Training and Consultancy Trade Inc. Learning Management System (LMS) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Learning Management System (LMS): through 2026-09-18.	6.5	More Details

CVE-2026-102798	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeREX Group ThemeREX Addons trx_addons allows Stored XSS.This issue affects ThemeREX Addons: from n/a through 2.46.0.	6.5	More Details
CVE-2026-100513	Contributor Cross Site Scripting (XSS) in CF7 Views – Complete Entry Management for Contact Form 7 <= 3.2.5 versions.	6.5	More Details
CVE-2026-55251	NetBox Device Type Library is a collection of community-sourced device type definitions for import into NetBox. Prior to commit f41fc1e, the CI workflow .github/workflows/validation.yml runs on pull_request and executes code supplied by the pull request before any maintainer review. Three PR-editable files drive this: "requirements.txt", ".pre-commit-hooks-config.yaml" / ".pre-commit-yamlfmt-config.yaml", and ".gitmodules". A contributor with no special repository access could open a pull request that modifies these files and have their code run on the CI runner. This issue has been patched via commit f41fc1e.	6.5	More Details
CVE-2026-102383	Missing Authorization vulnerability in VillaTheme Lookzy woo-lookbook allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Lookzy: from n/a through 1.1.14.	6.5	More Details
CVE-2026-103085	Improper Access Control vulnerability in WP User Manager WP User Manager wp-user-manager allows Privilege Abuse.This issue affects WP User Manager: from n/a through 2.9.20.	6.5	More Details
CVE-2026-82357	RT-Labs AB C-Open CANopen contains a NULL pointer dereference if the LSS protocol is used to configure the device. An object defined by the user application may not have all required subindexes for object 0x1018. An unauthenticated, remote attacker with access to the CAN bus, through a compromised node for instance, can initiate the LSS protocol on a device with a misconfigured identity object and potentially crash the device. Fixed in 1.1.1.	6.5	More Details
CVE-2026-82358	RT-Labs AB C-Open CANopen contains a write protection bypass in the SDO (Service Data Object) server implementation 'src/co_sdo_server.c' that fails to properly validate write permissions when processing download-segment frames. An unauthenticated attacker on the CAN bus can initiate an SDO upload for a read-only Object Dictionary (OD) entry, which sets a data pointer to the read-only object, then send download-segment frames to write to that memory location. The download-segment handler does not verify that a download session is active, allowing any CANopen node to overwrite read-only OD entries using two SDO frames. Note that CANopen protocol operates over CAN bus and does not provide built-in authentication mechanisms. Fixed in 1.1.1.	6.5	More Details
CVE-2026-103538	A security flaw has been discovered in ZongXR SuperMarket 1.0.0.0. Affected by this issue is the function OrderController.deleteOrder of the file order/src/main/java/com/supermarket/order/controller/OrderController.java of the component Order Deletion Endpoint. Performing a manipulation of the argument orderId results in missing authentication. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.5	More Details
CVE-2026-104459	YesWiki before 4.6.7 contains a server-side request forgery vulnerability in WebfingerService that allows unauthenticated attackers to trigger HTTPS requests to internal hosts. Attackers can POST a crafted actor_handle with a numeric host and port to the abonnements view to probe internal HTTPS services and ports.	6.5	More Details
CVE-2026-103086	Missing Authorization vulnerability in Stiofan UsersWP userswp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UsersWP: from n/a through 1.2.74.	6.5	More Details
CVE-2026-16596	The WP Directory Kit plugin for WordPress is vulnerable to generic SQL Injection via the 'data_fields_list' parameter in all versions up to, and including, 1.5.4 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 custom-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-2026-91109	The Simply Schedule Appointments plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.6.12.31 via the 'complete_group' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to disclose every co-booker's private per-appointment id_token (exposed as public_token) alongside their PII (name and email address), then use each leaked token to read, overwrite arbitrary appointment meta on, or cancel the co-booker's appointment via the same REST controller. Exploitation requires the attacker to possess a valid id_token for any single	6.5	More Details

	appointment within the targeted group booking.		
CVE-2026-100251	Wormhole.app as deployed before 2026-08-22 misconfigures the coturn TURN server and does not properly restrict TCP relay peers, allowing an unauthenticated attacker to access instance metadata or to source TCP connections from the Wormhole relay's IP.	6.5	More Details
CVE-2026-95264	Feehi CMS 2.1.1 is vulnerable to Directory Traversal. An authenticated backend user with article edit permission can delete arbitrary files writable by the PHP process. Article image metadata is used to construct a filesystem path and is passed to `unlink()` without path traversal or directory validation.	6.5	More Details
CVE-2026-104458	YesWiki before 4.6.7 contains a server-side request forgery vulnerability in validateKeyUrl() that allows unauthenticated attackers to bypass the SSRF guard using 6to4, NAT64, or IPv4-compatible IPv6 addresses. Attackers can send a crafted Signature keyId to the public actor inbox route to reach cloud metadata, loopback services, or internal hosts.	6.5	More Details
CVE-2026-39439	Missing Authorization vulnerability in Kiera Howe WebSamurai websamurai allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WebSamurai: from n/a through 1.0.7.	6.5	More Details
CVE-2026-104713	Allocation of resources without limits or throttling vulnerability in the Apache Struts REST plugin. A request body is read into memory without any bound on how much will be accepted, so a single request can cause the server to allocate memory in proportion to its size, exhausting the Java heap and denying service to other users. No additional setting has to be enabled. Applications that do not use the REST plugin are not affected. This issue affects Apache Struts: from 2.1.8 through 2.3.37, from 2.5.0 through 2.5.33, from 6.0.0 through 6.11.0, from 7.0.0 through 7.3.0. Users are recommended to upgrade to version 6.12.0 or 7.4.0, which fixes the issue.	6.5	More Details
CVE-2026-101881	OpenClaw Windows Node before 2026.7.1 contains an allocation of resources without limits vulnerability in the gateway WebSocket transport that allows connected gateways to exhaust node memory. Attackers can send an unending sequence of WebSocket continuation frames without EndOfMessage to cause unbounded memory growth until the node process crashes.	6.5	More Details
CVE-2026-62080	Contributor Cross Site Scripting (XSS) in Happy Addons for Elementor <= 3.23.1 versions.	6.5	More Details
CVE-2026-62079	Contributor Cross Site Scripting (XSS) in Qi Addons For Elementor <= 1.11 versions.	6.5	More Details
CVE-2026-103492	In JetBrains YouTrack before 2026.2.19422 doS attack was possible via crafted PSD attachments	6.5	More Details
CVE-2026-62078	Contributor Cross Site Scripting (XSS) in Premium Addons for Elementor <= 4.11.105 versions.	6.5	More Details
CVE-2026-12951	The Dc Woocommerce Multi Vendor plugin for WordPress is vulnerable to SQL Injection via the 'order_by' parameter of the /multivendorx/v1/compliance/report-abuse REST endpoint in versions up to and including 5.0.18. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query — the value is concatenated directly into an ORDER BY clause where esc_sql() (which only neutralizes characters needed to break out of quoted string literals) provides no protection. This makes it possible for authenticated attackers, with vendor-level access and above (users granted the 'edit_stores' capability), 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-2026-102991	Mako is a template library written in Python. Prior to 1.4.2, on Windows, TemplateLookup.get_template() in mako/lookup.py resolves template URIs with posixpath, while Template.__init__() in mako/template.py validates them with os.path, which uses ntpath. A URI beginning with a drive designator causes ntpath to absorb the traversal segments before the leading dot-dot check, while posixpath resolution can escape the configured template directory. An application that passes attacker-controlled template names or include paths can disclose process-readable files on the same volume, and a targeted file containing Mako template syntax may also be parsed and executed as a template. Raw URL paths are generally normalized before reaching this form, but query strings, form or JSON bodies, route parameters, and dynamic include expressions can preserve it. This issue is fixed in version 1.4.2.	6.5	More Details
CVE-	Velociraptor's SetClientMetadata used the wrong permission check to enforce setting metadata on the server. This allows a user with LABEL_CLIENTS permission to update the server metadata. Server		More

2026-78411	metadata is often used to store site wide configuration data that should only be updated by the server admin.	6.5	Details
CVE-2026-104449	YesWiki before 4.6.7 contains an access control vulnerability allowing unauthenticated attackers to overwrite any existing wiki page, including pages whose write ACL restricts editing, via the Bazar entry-creation flow. Attackers can submit a crafted entry with an attacker-controlled id_fiche matching an existing page, overwriting its body for mass defacement and content destruction.	6.5	More Details
CVE-2026-104450	YesWiki before 4.6.7 contains a missing authorization flaw in the pointimage action (tools/attach/actions/pointimage.php), which saves content to an attacker-chosen page with write ACL checks bypassed. Unauthenticated attackers can POST pagetag, title, and description fields to any page rendering {{pointimage}} to append raw HTML or JavaScript to any wiki page, including pages whose write ACL restricts editing, causing stored cross-site scripting in viewers' and administrators' browsers.	6.5	More Details
CVE-2026-42700	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Image Slider Widget image-slider-widget allows Stored XSS.This issue affects Image Slider Widget: from n/a through 1.1.130.	6.5	More Details
CVE-2026-32585	Missing Authorization vulnerability in airano Airano MCP Bridge airano-mcp-bridge allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Airano MCP Bridge: from n/a through 2.11.0.	6.5	More Details
CVE-2026-103337	Missing Authorization vulnerability in Kirillbdev WC Ukraine Shipping wc-ukr-shipping allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WC Ukraine Shipping: from n/a through 1.23.2.	6.5	More Details
CVE-2026-93995	Improper input validation in sshd-git in Apache MINA SSHD, versions up to 2.19.0 and 3.0.0-M1 to 3.0.0-M5. Apache MINA SSHD is a Java library for client-side and server-side SSH. Component org.apache.sshd:sshd-git provides though class GitPgmCommandFactory a way to configure an Apache MINA SSHD server such that authenticated SSH clients can remotely execute git commands via the JGit library on git repositories stored on the server. In CVE-2026-58624 this mechanism was restricted to only a few git commands, including "git archive" without "--output" or "-o" options such that the resulting archive would not be written on the server but instead sent back to the client over the SSH connection. The fix done for CVE-2026-58624 was insufficient as it missed removing the single-argument "-o=file.zip" version of the command parameter from the "archive" command. Users are recommended to upgrade to version 2.20.0 or 3.0.0-M6, which fix this issue.	6.5	More Details
CVE-2026-93996	Uncontrolled resource consumption in component sshd-scp in Apache MINA SSHD versions up to 2.19.0 or 3.0.0-M1 to 3.0.0-M5. Apache MINA SSHD is a Java library for client-side and server-side SSH. Component sshd-scp of Apache MINA SSHD provides a Java implementation of SCP. The SCP command protocol is line-oriented with LF-terminated lines. The protocol handler in sshd-scp did not impose any limit on the length of such protocol lines. A malicious peer just sending a junk command containing a never-ending sequence of characters but never a LF would cause the receiver to allocate memory to store this whole junk command, exhausting memory and crashing the application with an OutOfMemoryError. Users are recommended to upgrade to version 2.20.0 or 3.0.0-M6, which fix this issue by enforcing an upper limit on the length of SCP protocol lines.	6.5	More Details
CVE-2026-96835	Contributor Cross Site Scripting (XSS) in King Addons for Elementor <= 51.1.85 versions.	6.5	More Details
CVE-2026-101889	The Prime Mover plugin for WordPress before 2.2.1 contains a path traversal vulnerability that allows authenticated administrators to delete arbitrary directories by importing a crafted WPRIME/TAR package with manipulated tar_root_folder values in wprime-config.json. Attackers can exploit insufficient path validation in computeExtractVariables() and validateImportedSiteVsPackage() to cause primeMoverDoDelete() to remove directories outside the intended extraction path, potentially deleting critical WordPress directories such as wp-admin and rendering the site inoperable.	6.5	More Details
CVE-2026-103063	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpmet ElementsKit Elementor addons Lite elementskit-lite allows Stored XSS.This issue affects ElementsKit Elementor addons Lite: from n/a through 4.0.6.	6.5	More Details
CVE-2026-97067	Contributor Cross Site Scripting (XSS) in EWWW Image Optimizer <= 8.7.7 versions.	6.5	More Details
CVE-2026-102139	An authorization check in the large file exchange feature of Kiteworks Email Protection Gateway did not correctly establish that the requesting user was a party to the package being requested. An authenticated user of that optional feature could read the subject, message body, and attachments of	6.5	More Details

	packages they neither sent nor received.		
CVE-2026-71299	A flaw was found in Maestro. Its REST API write endpoints were registered without proper authentication middleware. This allows a remote attacker to perform unauthorized write operations, such as creating, modifying, or deleting consumers and resource bundles. This could lead to data integrity issues or a denial of service (DoS).	6.5	More Details
CVE-2026-84740	The Events Calendar WordPress plugin before 6.17.5.1 does not validate or sanitise data submitted to an unauthenticated AJAX action before merging it into its rendering context, allowing unauthenticated users to execute arbitrary shortcodes registered on the site.	6.5	More Details
CVE-2026-95865	The Beaver Builder Page Builder – Drag and Drop Website Builder plugin for WordPress is vulnerable to blind SQL Injection via 'fields[][value]' Parameter in all versions up to, and including, 2.11.0.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The vulnerable get_autosuggest_values AJAX endpoint is reachable by any Contributor who owns a draft post, as the required fl_ajax_update nonce is emitted into the block editor for any user who can edit a Beaver Builder post type.	6.5	More Details
CVE-2026-94539	The SupportCandy – AI Customer Support Ticket System & Live Chatbot Agent plugin for WordPress is vulnerable to time-based SQL Injection via the 'sort_by' parameter in all versions up to, and including, 3.5.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the authenticated attacker to hold both a Subscriber-level (or higher) WordPress role and a SupportCandy Agent account with the 'Assign Agents' permission configured.	6.5	More Details
CVE-2026-62084	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr User Submitted Posts allows Stored XSS. This issue affects User Submitted Posts: from n/a through 20260810.	6.5	More Details
CVE-2026-97634	The Event Tickets and Registration plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 5.29.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. A Contributor-level user can reach the vulnerable code path by supplying a post_id they authored, as the can_access_page() gate requires only post authorship rather than the edit_others_posts capability for post owners.	6.5	More Details
CVE-2026-102394	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor essential-addons-for-elementor-lite allows Stored XSS. This issue affects Essential Addons for Elementor: from n/a through 6.8.4.	6.5	More Details
CVE-2026-103064	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpmet ElementsKit Elementor addons Lite elementskit-lite allows Stored XSS. This issue affects ElementsKit Elementor addons Lite: from n/a through 4.0.6.	6.5	More Details
CVE-2026-97292	Author Cross Site Scripting (XSS) in YITH WooCommerce Tab Manager <= 2.15.0 versions.	6.5	More Details
CVE-2026-105696	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the get-page RPC accepts a share-link permission object with blanket read access but does not verify that the caller-selected page-id belongs to the link's authorized pages set. An attacker with both a valid share link and the attacker's own authenticated Penpot session can retrieve the complete shape and design data of another page in the same file when its identifier is known, because get-page requires authentication. The related get-file-fragment RPC also permits share-link access without mapping fragments to authorized pages. This issue is fixed in version 2.18.0.	6.5	More Details
CVE-2026-103339	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpmet Metform metform allows Stored XSS. This issue affects Metform: from n/a through 4.3.0.	6.5	More Details
CVE-2026-105681	Ghost is a Node.js content management system. From 5.9.0 until 6.44.1, an input validation issue allowed members to access comments they were not authorized to access. This issue is fixed in version 6.44.1.	6.5	More Details

CVE-2026-103343	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP ManageNinja LLC FluentForm fluentform allows Stored XSS.This issue affects FluentForm: from n/a through 6.2.14.	6.5	More Details
CVE-2026-105680	Ghost is a Node.js content management system. From 5.81.0 until 6.60.0, staff with the Author role could delete posts and pages that they did not author. This issue is fixed in version 6.60.0.	6.5	More Details
CVE-2026-89039	A caller who can invoke the convert_playwright_script prompt in mcp-k6 can pass a bare file path as the playwright_script argument and receive the contents of any file readable by the user running the server, including SSH keys and cloud credentials in that user's home directory (path traversal). The working-directory restriction applied to '@'-prefixed paths can also be bypassed with a symbolic link inside the working directory that points outside it.	6.5	More Details
CVE-2026-97301	Contributor Cross Site Scripting (XSS) in Cool Formkit Lite <= 2.7.8 versions.	6.5	More Details
CVE-2026-88397	ApiAdmin v.5.0 and before is vulnerable to SQL Injection in the user-list endpoint GET /admin/User/getUsers via the gid parameter.	6.5	More Details
CVE-2026-103679	A flaw was found in tnep. A remote attacker could exploit this vulnerability by providing a specially crafted Transport Neutral Encapsulation Format (TNEF) file containing multiple message bodies. During extraction, improper memory management triggers a use-after-free and double-free condition, causing the application to crash and resulting in a Denial of Service (DoS).	6.5	More Details
CVE-2026-102805	A flaw has been found in Nothings stb up to 1.16. This affects the function stbi_write_png_to_mem/stbi_write_jpg_core/stbi_write_tga_core in the library stb_image_write.h of the component Image Encoding. Executing a manipulation can lead to integer overflow. The attack can be executed remotely. The exploit has been published and may be used.	6.5	More Details
CVE-2026-105069	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nikki Blight QR Redirector qr-redirector allows Stored XSS.This issue affects QR Redirector: from n/a through 2.0.5.	6.5	More Details
CVE-2026-105064	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Parameter Injection.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.22.	6.5	More Details
CVE-2026-102393	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Starter Templates astra-sites allows Stored XSS.This issue affects Starter Templates: from n/a through 4.7.7.	6.5	More Details
CVE-2026-102914	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Presto Player presto-player allows Stored XSS.This issue affects Presto Player: from n/a through 4.5.2.	6.5	More Details
CVE-2026-103084	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LeapWorx Premium Addons for Elementor premium-addons-for-elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.11.109.	6.5	More Details
CVE-2026-102804	A vulnerability was detected in Nothings stb up to 2c980bb59875b0d32144a71867fbdebb2f77cd20. The impacted element is the function hexwave_init in the library stb_hexwave.h. Performing a manipulation of the argument width/oversample results in integer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.5	More Details
CVE-2026-104386	Missing Authorization vulnerability in WPFunnels Team WP VR wpvr allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP VR: from n/a through 9.1.3.	6.5	More Details
CVE-2026-104396	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Peters Name Directory name-directory allows Stored XSS.This issue affects Name Directory: from n/a through 1.34.2.	6.5	More Details
CVE-2026-100279	In JetBrains YouTrack before 2026.2.19197 changing an integration URL exposed its stored credentials	6.5	More Details

CVE-2026-104400	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Blocks b-blocks allows Stored XSS.This issue affects B Blocks: from n/a through 2.1.8.	6.5	More Details
CVE-2026-104404	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP GiveWP give allows Stored XSS.This issue affects GiveWP: from n/a through 4.17.0.	6.5	More Details
CVE-2026-100274	In JetBrains YouTrack before 2026.2.19197 project Admin could trigger DoS via a notification template	6.5	More Details
CVE-2026-104409	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Image Photo Gallery Final Tiles Grid final-tiles-grid-gallery-lite allows Stored XSS.This issue affects Image Photo Gallery Final Tiles Grid: from n/a through 3.6.13.	6.5	More Details
CVE-2026-103288	Ghost, an open-source publishing platform, contains an input validation flaw in its comment like feature in versions from 5.9.0 before 6.44.1. An authenticated member can delete comment likes or dislikes belonging to other users that they are not authorized to delete, resulting in an authorization bypass and unauthorized modification of comment engagement data.	6.5	More Details
CVE-2026-103289	Ghost from 5.9.0 before 6.44.1 contains an input validation issue in the comments feature that allows authenticated members to access comments they are not authorized to view, resulting in disclosure of restricted comment data.	6.5	More Details
CVE-2026-104673	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sonaar MP3 Audio Player for Music, Radio & Podcast by Sonaar mp3-music-player-by-sonaar allows Stored XSS.This issue affects MP3 Audio Player for Music, Radio & Podcast by Sonaar: from n/a through 5.14.2.	6.5	More Details
CVE-2026-105056	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode eCommerce Product Catalog ecommerce-product-catalog allows Stored XSS.This issue affects eCommerce Product Catalog: from n/a through 3.6.2.	6.5	More Details
CVE-2026-100152	The The All in One SEO - AI SEO Plugin to Boost SEO Rankings & Traffic (Schema, Local SEO, Sitemap & SEO Insights) plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.0.2 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. This requires the AIOSEO breadcrumb to be rendered on the search results page via the block, widget, shortcode, or template tag.	6.5	More Details
CVE-2026-105060	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Logo Showcase logo-showcase allows Stored XSS.This issue affects Logo Showcase: from n/a through 4.0.4.	6.5	More Details
CVE-2026-97298	Contributor Cross Site Scripting (XSS) in King Addons for Elementor <= 51.1.86 versions.	6.5	More Details
CVE-2026-100143	The FluentCart A New Era of eCommerce WordPress plugin before 1.6.5 does not verify that the person placing a guest checkout controls the email address supplied, allowing unauthenticated attackers who know an existing guest customer's email to obtain a logged-in account bearing that address together with the customer's stored record.	6.5	More Details
CVE-2026-93474	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	6.5	More Details
CVE-2026-97247	Unauthenticated Broken Access Control in Blocksy Companion <= 2.1.55 versions.	6.5	More Details
CVE-2026-104969	Plane is an open-source project management tool. Prior to 1.4.0, the cycle-issues endpoint accepts issue UUIDs in the request body without validating that they belong to the caller's workspace. An authenticated user can add issues from any workspace to a cycle they control. If a victim issue is already assigned to a cycle, the operation removes it from the victim's cycle, causing a destructive cross-tenant write. This issue is fixed in 1.4.0.	6.5	More Details
CVE-2026-	Unauthenticated Insecure Direct Object References (IDOR) in Bus Ticket Booking with Seat Reservation <= 5.9.3 versions.	6.5	More Details

97251			
CVE-2026-97258	Subscriber Broken Access Control in Aruba Migration Tool <= 1.0.4 versions.	6.5	More Details
CVE-2026-82045	UTMStack before 11.2.16 contains a JPQL injection vulnerability that allows authenticated attackers to read arbitrary entity data by exploiting UtmNetworkScanService.searchPropertyValues(), which builds a JPQL query with String.format() and executes it via em.createQuery() without parameter binding. Attackers can inject malicious JPQL through the value parameter in the GET /api/utm-network-scans/searchPropertyValues endpoint to extract sensitive data including credential tables such as jhi_user.	6.5	More Details
CVE-2026-97269	Unauthenticated Insecure Direct Object References (IDOR) in WPFunnels <= 3.13.1 versions.	6.5	More Details
CVE-2026-105113	Nezha Dashboard from 1.8.0 before 2.3.13 contains an improper locking vulnerability where a non-deferred mutex unlock leaks on a nil-map panic path. Any authenticated non-admin member can issue four notification API calls to permanently deadlock the alerting subsystem, then exhaust memory with blocking requests.	6.5	More Details
CVE-2026-97280	Missing Authorization vulnerability in Mamunur Rashid Review Schema review-schema allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Review Schema: 3.1.0.	6.5	More Details
CVE-2026-79900	boks_ksllgsd accepts a checksum algorithm name in the MD field of an authenticated KSL start message. Affected releases verify that OpenSSL recognizes the digest name but do not verify that the value fits in a fixed 16-byte checksum context field before copying it. An authenticated KSL client can supply an oversized, OpenSSL-recognized digest name and write beyond the end of the heap allocation.	6.5	More Details
CVE-2026-103036	oRPC is a tool that helps build APIs that are end-to-end type-safe and adhere to OpenAPI standards. Prior to 1.14.9, the @orpc/json-schema SmartCoercionPlugin uses JsonSchemaCoercer to collect object properties in a plain object and to resolve schema.properties entries through the prototype chain. A remote client that can reach a procedure with an object input schema can supply __proto__ to replace the prototype of the single coerced request object, or supply Object.prototype member names such as constructor and toString so inherited values are treated as sub-schemas and pass the coercer's satisfaction check. Attacker-controlled inherited properties can consequently affect handler, Object.assign, or configuration lookups, while legitimate __proto__ properties are dropped. The global Object.prototype, unrelated objects, other requests, and other users are not modified, and downstream schema validation still runs. This issue is fixed in version 1.14.9.	6.5	More Details
CVE-2026-103505	Improper neutralization of argument delimiters in the volume handling component in AWS EFS CSI Driver (aws-efs-csi-driver) v3.1.0 through v3.4.2 might allow remote authenticated users with PersistentVolume creation permissions to inject arbitrary mount options via comma-separated values in the mounttargetipmap volumeAttribute. To remediate this issue, users should upgrade to version v3.5.0 or later.	6.5	More Details
CVE-2026-97239	Subscriber Broken Access Control in MCP Content Manager Lite <= 1.1.0 versions.	6.5	More Details
CVE-2026-19856	The All in One SEO WordPress plugin before 5.0.2.1 does not correctly determine which shortcodes are present in content derived from user input before deciding which ones to strip, allowing unauthenticated users to execute arbitrary shortcodes registered on the site. On sites upgraded from older versions the protection is disabled outright, making the issue reachable without any crafted input.	6.5	More Details
CVE-2026-105306	A flaw was found in the Dynamic Client Registration flow of the Keycloak identity and access management server. The issue occurs because the registration process fails to filter security-sensitive client attributes when a new client is created. An attacker with a valid Initial Access Token can register a client that bypasses audience checks during token introspection. This allows the attacker to view sensitive identity information, roles, and session details from access tokens belonging to other applications in the same realm.	6.5	More Details
CVE-2026-97236	Subscriber Cross Site Scripting (XSS) in ThemeREX Addons < 2.45.0 versions.	6.5	More Details
	oRPC is a tool that helps build APIs that are end-to-end type-safe and adhere to OpenAPI standards.		

CVE-2026-103918	Prior to 1.14.10, the @orpc/zod ZodSmartCoercionPlugin and experimental_ZodSmartCoercionPlugin collect object and record properties in plain objects and resolve shape keys through the prototype chain. A remote client that can reach a procedure with an object or record input can supply __proto__ to replace the prototype of the returned request object, allowing attacker-controlled inherited values to reach application lookups. For object schemas, keys such as constructor, toString, and __proto__ can instead resolve inherited members as Zod schemas and cause an unhandled TypeError before validation. The global Object.prototype, unrelated objects, other requests, and other users are not modified, and the availability effect is limited to crafted requests rather than persistent process-wide state. This issue is fixed in version 1.14.10.	6.5	More Details
CVE-2026-102375	Subscriber Broken Access Control in Optimole <= 4.2.14 versions.	6.5	More Details
CVE-2026-97279	Contributor Cross Site Scripting (XSS) in Polylang <= 3.8.9 versions.	6.5	More Details
CVE-2026-97288	Contributor Cross Site Scripting (XSS) in OAuth Server <= 4.5.1 versions.	6.5	More Details
CVE-2026-97270	Subscriber Cross Site Scripting (XSS) in CMB2 <= 2.13.0 versions.	6.5	More Details
CVE-2026-104962	Plane is an open-source project management tool. Prior to 1.4.0, GET /api/v1/workspaces/{slug}/projects/{project_id}/members/ returns the complete project-member roster, including each member's email address, first and last name, display name, avatar, and role. ProjectMemberPermission gates the endpoint, but its SAFE_METHODS branch checks only whether the caller is an active ProjectMember of any project in the workspace and does not bind the check to view.project_id. The view then filters solely by the project_id supplied in the URL. Consequently, any authenticated user who belongs to one project in a workspace, including a Guest, can read the roster of another private project in the same workspace. This issue is fixed in 1.4.0.	6.5	More Details
CVE-2026-104960	Plane is an open-source project management tool. Prior to 1.4.0, Plane exposes the workspace-scoped GET /api/assets/v2/workspaces/{workspace_slug}/download/{asset_id}/ endpoint for project-bound FileAsset objects without enforcing access to the asset's owning project. An authenticated user who belongs to the same workspace, is not a member of the victim's secret project, and knows the target asset UUID can receive a 302 redirect to a signed download URL. The intended project-scoped route for the same asset correctly returns 403. Confirmed affected project-bound asset types are ISSUE_ATTACHMENT, COMMENT_DESCRIPTION, PAGE_DESCRIPTION, and PROJECT_COVER. This bypass exposes private file content protected by the secret project boundary. This issue is fixed in 1.4.0.	6.5	More Details
CVE-2026-97266	Contributor Cross Site Scripting (XSS) in Virtue/Ascend/Pinnacle Toolkit <= 4.9.12.1 versions.	6.5	More Details
CVE-2026-97262	Contributor Cross Site Scripting (XSS) in Visual Composer Website Builder <= 45.16.2 versions.	6.5	More Details
CVE-2026-97286	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Strong Testimonials strong-testimonials allows Stored XSS.This issue affects Strong Testimonials: from n/a through 3.3.11.	6.5	More Details
CVE-2026-102146	An authenticated Email Protection Gateway administrator holding only limited, delegated permissions could write files with attacker-controlled content to arbitrary locations accessible to the Email Protection Gateway service account. This exceeds the administrator's intended privileges and could be used to alter application files and configuration or to disrupt the availability of the service.	6.5	More Details
CVE-2026-92712	The ReactPress – Create React App for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'permalink' parameter in all versions up to, and including, 3.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because the permalink parameter is only passed through sanitize_url(), which does not prevent fetching attacker-controlled remote URLs whose response body — including script tags and event-handler attributes — is written verbatim to disk via file_put_contents().	6.4	More Details

CVE-2026-90992	The Redux Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via User Meta Merge via 'user-mediaurl' Media Field in all versions up to, and including, 4.5.14 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. This is exploitable by Subscriber-level users who can store a payload in user meta fields such as the biography, session_tokens (via a crafted User-Agent at login), or persisted_preferences (via the REST API), which are then promoted to the site-wide redux_demo option when a media URL repair is triggered on the demo panel.	6.4	More Details
CVE-2026-15795	The Responsive Plus – Elementor Templates & Starter Sites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 3.5.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-100148	The Rich Showcase for Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'reviews[.].text' parameter in all versions up to, and including, 7.1.3 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. The payload is delivered entirely through a Google review posted for the connected business and requires no WordPress account; the plugin's default daily cron auto-imports the malicious review text, and execution triggers for every visitor on DOMContentLoaded without any further user interaction.	6.4	More Details
CVE-2026-101162	The WP Ultimate Review WordPress plugin before 2.4.4 does not escape some of its review overview settings before outputting them in posts, which could allow users with a role as low as author to perform Stored Cross-Site Scripting attacks, when author reviews are enabled.	6.4	More Details
CVE-2026-6171	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'target' parameter of the plugin's bt_bb_icon shortcode in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6170	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'images' parameter of the plugin's bt_bb_css_image_grid shortcode in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-47565	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a privileged user could trigger a race condition that leads to an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.4	More Details
CVE-2026-103291	Ghost versions from 3.20.2 before 6.51.0 contain a server-side request forgery vulnerability in image dimension refetching that allows authenticated staff users to trigger outbound HTTP requests to arbitrary URLs. Attackers can point image cards at attacker-controlled hosts or internal network endpoints to access metadata services and internal resources unavailable from the public internet.	6.4	More Details
CVE-2026-89424	The Duplicate Post plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noti_token' parameter in all versions up to, and including, 1.5.6 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. This requires that the site owner has enabled the plugin's User Level Permissions for the Subscriber role, as this grants access to the i_saw_this_noti AJAX branch needed to deliver the payload.	6.4	More Details
CVE-2026-86610	The Download Manager WordPress plugin before 3.3.71 does not sufficiently sanitise and escape a package setting before outputting it back in a page, which could allow users with the Author role and above to perform Stored Cross-Site Scripting attacks against any visitor who opens the package's download dialogue, including administrators. Only sites running PHP below 8.1 are affected, as the sanitisation applied when the setting is saved does not neutralise single quotes there.	6.4	More Details
CVE-2025-14564	The Viable URL Media Uploader plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
	The Real Estate Manager – Property Listing and Agent Management plugin for WordPress is vulnerable		

CVE-2026-93908	to Stored Cross-Site Scripting via the 'before_price_text' parameter in all versions up to, and including, 7.3 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. The vulnerability is further enabled by the absence of any capability, nonce, or ownership check on the wp_ajax_rem_create_pro_ajax handler, and because the value is persisted via update_post_meta rather than post_content, the wpkses filtering tied to the unfiltered_html capability does not apply.	6.4	More Details
CVE-2025-12828	The Ultra Addons Lite for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Type Out widget in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-96268	The Awesome Support – WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gdpr-data' parameter in all versions up to, and including, 6.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is exploitable by Subscriber-level users against other accounts because the AJAX handlers accept an arbitrary gdpr-user ID without verifying it belongs to the requester, and the required wpas-gdpr-nonce is emitted via wp_localize_script to every logged-in user on frontend plugin pages and on /wp-admin/profile.php.	6.4	More Details
CVE-2026-101925	The bbp style pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name (via /wp-admin/profile.php) + bbp_reply_content (via bbPress reply form)' parameter in all versions up to, and including, 6.4.8 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. Successful exploitation requires the attacker to wrap their crafted reply in a <pre> block, which prevents WordPress's wpautop/wptexturize processors from converting straight double quotes in the stored display name into typographic curly-quote entities that would otherwise neutralize the attribute-injection.	6.4	More Details
CVE-2026-94378	The SupportCandy – AI Customer Support Ticket System & Live Chatbot Agent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 3.5.3 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. This exploit chain requires the 'Register user if not exists' setting to be disabled, which is its default configuration.	6.4	More Details
CVE-2026-71298	A flaw was found in maestro. A remote attacker could exploit a SQL injection vulnerability in the `orderBy` query parameter of its REST API list endpoints. This flaw, which does not require authentication, allows for read-only blind extraction of data from the database.	6.4	More Details
CVE-2026-97876	A local attacker with control over GRUB's configuration can bypass lockdown restrictions when booting with Secure Boot and load an unsigned GRUB module, while GRUB continues to report lockdown is enabled. The vulnerability is caused by insufficient validation of the MMIO base address passed to the GRUB serial command. GRUB does not validate that the base address corresponds to a UART device, rather than being an arbitrary memory address. This allows an attacker to trick GRUB into writing non-arbitrary data at an attacker-controlled address, including resetting the grub_file_verifiers list in a way that disables the subsequent verification of loaded modules.	6.4	More Details
CVE-2026-6172	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'caption' parameter of the plugin's bt_bb_image shortcode in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-6173	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'background_image' parameter of the plugin's bt_bb_section shortcode in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-92767	The Twenty20 Image Before-After plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'offset' Shortcode Attribute in all versions up to, and including, 2.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user	6.4	More Details

	accesses an injected page.		
CVE-2026-102797	Server-Side Request Forgery (SSRF) vulnerability in ThemeREX Group ThemeREX Addons trx_addons allows Server Side Request Forgery.This issue affects ThemeREX Addons: from n/a through 2.46.0.	6.4	More Details
CVE-2026-97338	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Display Name in all versions up to, and including, 3.3.70 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. This requires the [wpdm_edit_profile] shortcode to be present on a front-end page accessible to Subscriber-level users, who can then submit a multiply entity-encoded payload via the display name field to bypass sanitization.	6.4	More Details
CVE-2026-97344	The Wp Social Login and Register Social Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Avatar Alt Attribute via Arbitrary User Meta Write in all versions up to, and including, 3.2.1 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. This requires the attacker to chain two steps: invoking the nonce-only dismiss_ajax_call endpoint (nonce accessible to Subscribers via any wp-admin page) to set the xs_social_profile_image meta flag on their own account, which activates the unescaped img output branch in xs_social_get_avatar, and then setting their display name to a script payload that core's ENT_NOQUOTES handling preserves unescaped.	6.4	More Details
CVE-2026-47586	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel module where an attacker could cause a use-after-free. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	6.4	More Details
CVE-2026-92727	The EmbedPress – PDF Embedder, 3D PDF FlipBook, Google Reviews, YouTube Videos, Upload & Embed PDF documents plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'slidesShow' Block Attribute in all versions up to, and including, 4.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The slidesShow block attribute is interpolated into an unquoted data-carousel-options HTML attribute, allowing a payload containing spaces to break out of the attribute and inject additional DOM attributes such as onfocus event handlers onto the wrapper element.	6.4	More Details
CVE-2026-96647	The Listdom: AI-powered Business Directory with Classifieds Ads Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'lsd[remark]' Parameter in all versions up to, and including, 6.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is exploitable by Subscriber-level users because the listing-creation branch of the AJAX handler omits a capability check, and the required nonce is publicly emitted on any page containing the [listdom-dashboard] shortcode.	6.4	More Details
CVE-2026-88037	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `title` attribute of the `bt_bb_service` shortcode in all versions up to, and including, 5.7.2. 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-2026-11895	The HT Mega Addons for Elementor – Elementor Widgets & Template Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Data Table 'display_options' Setting in all versions up to, and including, 3.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-96256	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Map block's 'marker' attribute in versions up to, and including, 6.4.5 This is due to insufficient input sanitization and output escaping on marker title/content values, which are stored as JSON and then decoded and concatenated directly into raw HTML by the frontend script's InfoWindow content builder. 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-2026-14876	The Smart Slider 3 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data-href' parameter in all versions up to, and including, 3.5.1.38 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-2026-105389	A security vulnerability has been detected in feelec-yishu feelcrm-os 1.0.0. This issue affects some unknown processing of the file App/Feelcrm/Crm/Controller/UploadController.class.php of the component UploadTicketFile Endpoint. Such manipulation of the argument cmd leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-105168	A vulnerability was identified in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. This affects an unknown function of the file admin/admin.php of the component Order Assignment Block. The manipulation of the argument order_id/delivery_person_id leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-104054	A security flaw has been discovered in calcom cal.diy up to 6.2.0. This affects the function doesUserIdHaveAccessToBooking of the file BookingAccessService.ts of the component PBAC Permission Engine. Performing a manipulation results in missing authorization. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	6.3	More Details
CVE-2026-105171	A security vulnerability has been detected in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. Affected by this vulnerability is an unknown functionality of the file admin/admin.php of the component Role Attribute Handler. Such manipulation of the argument Name leads to authorization bypass. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. Multiple endpoints are affected. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-102136	In multi-node deployments, an attacker who had already obtained code execution on one appliance node could submit a value through an internal cluster interface that was written into monitoring configuration on another node without sufficient validation, potentially allowing OS commands to be executed there. Execution was limited to an unprivileged service account on that node.	6.3	More Details
CVE-2026-105388	A weakness has been identified in feelec-yishu feelcrm-os 1.0.0. This vulnerability affects the function index of the file App/Feelcrm/Index/Controller/MemberController.class.php of the component Member Endpoint. This manipulation of the argument group_id causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-104053	A vulnerability was identified in itsourcecode Pet Shop Management System 1.0. The impacted element is an unknown function of the file admin_reservefilter.php. Such manipulation of the argument filter leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-105165	A vulnerability has been found in devopspolis secrets-replicator up to 0.4.0. Impacted is the function process_single_secret of the file src/handler.py of the component AssumeRole Handler. Such manipulation of the argument external_id leads to incorrect permission assignment. The attack can be executed remotely. Upgrading to version 0.5.0 is recommended to address this issue. The name of the patch is b42239405fbf4fae3c3f0048fc0b4225112edceb. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-105444	A security flaw has been discovered in dotnet eShop .NET 8. The impacted element is the function GetOrderAsync of the file src/Ordering.API/Apis/OrdersApi.cs of the component Ordering API. Performing a manipulation of the argument OrderNumber results in improper control of resource identifiers. The attack is possible to be carried out remotely. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-102842	A vulnerability was identified in gedelumbung HospitalManagement up to c2d45543789a3887067d3915f69d44cfc2cf76a8. Affected by this issue is the function app_user_login_model.php::cekUserLogin of the file application/models/app_user_login_model.php of the component KCFinder File Manager. Such manipulation of the argument ADMIN_RS_KCFINDER leads to unrestricted upload. It is possible to launch the attack remotely. The exploit is publicly available and might be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
	A vulnerability was determined in itsourcecode Pet Shop Management System 1.0. The affected		

CVE-2026-104052	element is an unknown function of the file admin_reject_completed.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-102906	A vulnerability was identified in 0xshariq github-mcp-server up to 52e764a7d66eac1726fce02ca7bb5a638571801a. This issue affects the function child_process.exec of the file src/github.ts of the component Git Remove MCP Tool. Such manipulation of the argument File leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-104606	A security flaw has been discovered in itsourcecode Online Admission System Project 1.0. The impacted element is an unknown function of the file confirm.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-96821	Subscriber Privilege Escalation in FluentBoards <= 2.0.12 versions.	6.3	More Details
CVE-2026-103534	A vulnerability was determined in David-Crty databasement up to 1.7.1. Affected is the function SnapshotPolicy.viewAny/SnapshotPolicy.view of the file /api/v1/snapshots of the component Snapshot Model. This manipulation causes improper access controls. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.7.2 is able to address this issue. The affected component should be upgraded.	6.3	More Details
CVE-2026-105287	A flaw has been found in feelec-yishu feelcrm-os 1.0.0. Affected is an unknown function of the file App/Feelcrm/Crm/Controller/AjaxRequestController.class.php of the component getMemberByGroups Endpoint. This manipulation of the argument groups[] causes sql injection. The attack is possible to be carried out 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.	6.3	More Details
CVE-2026-97281	Subscriber Broken Access Control in WP Project Manager <= 4.0.7 versions.	6.3	More Details
CVE-2026-104983	A vulnerability has been found in Linux Mint Xreader up to 4.6.9. Impacted is the function g_file_get_child of the file shell/ev-window.c of the component PDF Attachment Saving Handler. Such manipulation of the argument attachment leads to path traversal. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. One of the project maintainers closed this issue as "completed", because "EPUB support was removed from Xreader and reimplemented in Xepub". Code analysis indicates that this might be a misunderstanding of the situation.	6.3	More Details
CVE-2026-102505	Imager versions before 1.037 for Perl overflow a heap buffer fetching float samples from a paletted image in i_gsampf_fp. For a paletted image, getsamples() with type "float" allocates a buffer of one sample per pixel and fetches every requested channel of each pixel into it. Requesting more than one channel writes past its end. An attacker-supplied image controls the overflowing bytes through its palette.	6.3	More Details
CVE-2026-105329	A vulnerability was determined in TallCMS up to 4.8.0. This affects an unknown function of the file packages/tallcms/cms/src/Filament/Pages/ThemeManager.php of the component PluginManager. Executing a manipulation can lead to code injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called fdc18f4c6a36134f8986ca1d7e4e97092e3deb93. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-103226	A vulnerability was identified in Artifex Ghostscript up to 10.09.0. Affected is the function type1_callsubr of the file devices/vector/gdevpsfx.c of the component Pdfwrite. The manipulation leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. It is suggested to install a patch to address this issue. A solution was implemented: "I've chosen to fix this slightly differently by using the defined macro in the font parsing loop rather than in the callsubr function, because this better matches the pattern of 'normal' usage."	6.3	More Details
CVE-2026-103227	A weakness has been identified in GPAC up to 26.07.0. Affected by this issue is the function gf_dash_resolve_url of the file src/media_tools/dash_client.c of the component DASH Client. This manipulation causes buffer overflow. The attack is possible to be carried out remotely. Upgrading to version abi-16.26 can resolve this issue. Patch name: 4c8e26f278ff63eec57968f7bc696f604bb0cfd. It	6.3	More Details

	is recommended to upgrade the affected component.		
CVE-2026-77802	In Progress® Telerik® Fiddler® Classic for Windows, versions prior to v6.0.20262.10021, HTTP request smuggling is possible in the proxy request forwarding component. Requests containing multiple Content-Length headers with conflicting values are forwarded verbatim to the origin server, while Fiddler frames the request body using only the first Content-Length value. A local threat actor with low privileges who is able to send requests through the same Fiddler proxy instance as another user can exploit this desynchronization against a non-RFC-9110-compliant origin server that keeps the connection alive to smuggle an additional request. Because Fiddler returns the server connection to its pipe pool after reading only the first response, the unread smuggled response remains buffered on the socket and is served to the next session that reuses that connection, allowing the attacker to poison responses delivered to other users and to obtain responses intended for them.	6.3	More Details
CVE-2026-105286	A vulnerability was detected in Totolink A3002MU 1.0.0-B20230403.1455. This impacts the function sub_44B250 of the file /boafrm/formUploadFile of the component File Upload Handler. The manipulation of the argument filename results in path traversal. The attack can be executed remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-103544	A vulnerability was found in datadrivenconstruction OpenConstructionERP up to 14.8.1. The impacted element is an unknown function of the file backend/app/modules/ai/ai_client.py of the component AI Provider Configuration Handler. Performing a manipulation results in exposure of data element to wrong session. The attack may be initiated remotely. The exploit has been made public and could be used. Upgrading to version 15.0.0 is sufficient to resolve this issue. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-105254	A vulnerability was identified in itsourcecode Online Admission System 1.0. Impacted is an unknown function of the file /admin/schoolyear.php. Such manipulation of the argument sy leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-105251	A vulnerability was detected in vgmstream up to r2117. Affected by this vulnerability is the function ps_find_padding of the file src/coding/psx_decoder.c of the component VAG File Handler. Performing a manipulation results in out-of-bounds read. The attack is possible to be carried out remotely. The patch is named 4b8316652a30d40f99ad43310bed273fd1f8a7a3. It is suggested to install a patch to address this issue.	6.3	More Details
CVE-2026-105248	A security flaw has been discovered in vgmstream up to r2117. This affects the function parse_params/txtp_parse of the file src/meta/txtp_parser.c of the component TXTP File Handler. The manipulation results in out-of-bounds write. The attack may be launched remotely. The patch is identified as 4669d37a6af94866f6f0628678f9f0d46954e8b. It is best practice to apply a patch to resolve this issue.	6.3	More Details
CVE-2026-103233	A security vulnerability has been detected in AdithyaYelloju Restaurant-Management-System up to 7f0e7e84255e8fcfd488e83f8f91451bbbff6b9c. This impacts an unknown function of the file /admin/ of the component Admin Area. Such manipulation of the argument ID leads to authorization bypass. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-103254	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 contain a path traversal vulnerability in signed resume URL generation for Send-and-Wait approvals. Attackers with workflow creation permissions can mint valid approval URLs for gates in projects they cannot access by exploiting unresolved traversal sequences in caller-controlled node IDs, enabling cross-project approval forgery.	6.3	More Details
CVE-2026-105181	A vulnerability was identified in itsourcecode Online Admission System 1.0. This issue affects some unknown processing of the file register1.php. The manipulation of the argument fname leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-92923	The Unlimited Elements for Elementor WordPress plugin before 2.0.21 does not sanitise and escape a parameter before using it in a SQL statement, allowing users with a role as low as subscriber to perform blind SQL injection attacks and read arbitrary data from the database. Version 2.0.18 removed the subscriber-level access, so from 2.0.18 onward the issue requires a Contributor role or above.	6.3	More Details
CVE-2026-105233	A vulnerability has been found in kishor-23 food-waste-management-system 411989e3ecb82895e53dca7865f72145f03d7d93/b3a70b2c492dc9904de5be1ad9389bd79b87f82c. This affects an unknown function of the file login.php of the component Login Flow. Such manipulation of the argument PHPSESSID leads to session fixiation. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the	6.3	More Details

	problem early through an issue report but has not responded yet.		
CVE-2026-103690	A flaw has been found in itsourcecode Leave Management System 1.0. This vulnerability affects unknown code of the file /module/leave/controller.php. Executing a manipulation of the argument LEAVEID can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	6.3	More Details
CVE-2026-105180	A vulnerability was determined in Jeebase 0.0.1. This vulnerability affects the function updateUser of the file /user/update/info of the component UserService. Executing a manipulation of the argument user/tempUser can lead to dynamically-determined object attributes. The attack can be executed 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-2026-103116	A weakness has been identified in OS4ED openSIS-Classic up to 9.3. This impacts the function DBQuery of the file functions/GetStuListFnc.php of the component Student List Search Endpoint. This manipulation of the argument LO_sort causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-103543	A vulnerability has been found in itsourcecode Leave Management System 1.0. The affected element is an unknown function of the file /module/leavetype/controller.php. Such manipulation of the argument LEAVTID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-103114	A vulnerability was identified in OS4ED openSIS-Classic up to 9.3. The impacted element is the function DBQuery_assignment of the file modules/grades/Assignments.php of the component Assignment Management Endpoint. The manipulation of the argument Tables leads to sql 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.	6.3	More Details
CVE-2026-105141	A security flaw has been discovered in topoteretes cognee up to 1.5.4. The affected element is the function get_user_id_by_email of the file cognee/modules/users/authentication/get_api_auth_backend.py of the component JWT Signing Key Handler. The manipulation of the argument FASTAPI_USERS_JWT_SECRET results in hard-coded credentials. The attack may be launched remotely. Upgrading to version 1.6.0 is sufficient to fix this issue. The patch is identified as fa65fc0cd86cdba48d19aa76e36be862be982f5d. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-104613	A vulnerability was determined in CodeAstro Simple Pharmacy Management System 1.0. This vulnerability affects unknown code of the file /SimplePharmacy-PHP/product/view.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-103541	A vulnerability was detected in formtools.org Form Tools up to 3.1.1. This issue affects the function Files::uploadFile of the file global/code/actions.php of the component Ajax Handler. The manipulation results in unrestricted upload. It is possible to launch the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-104614	A vulnerability was identified in CodeAstro Simple Pharmacy Management System 1.0. This issue affects some unknown processing of the file /SimplePharmacy-PHP/product/delete.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-105186	A flaw has been found in itsourcecode Online Admission System 1.0. This impacts an unknown function of the file /new.php. Executing a manipulation of the argument schedid can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-105187	A vulnerability has been found in itsourcecode Online Admission System 1.0. Affected is an unknown function of the file /admin/key.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-104625	A security flaw has been discovered in CodeAstro Simple Loan Management System 1.0. Impacted is an unknown function of the file /admin/index.php. Performing a manipulation of the argument g_name 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-	A security flaw has been discovered in OS4ED openSIS-Classic up to 9.3. This affects an unknown function of the file functions/CustomFieldsFnc.php of the component Student Search. The manipulation of the argument cust results in sql injection. It is possible to launch the attack remotely. The exploit has	6.3	More

103115	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.		Details
CVE-2026-103540	A security vulnerability has been detected in formtools.org Form Tools up to 3.1.1. This vulnerability affects the function Clients::updateClientSettingsTab of the file global/code/Clients.class.php of the component Client Settings. The manipulation of the argument page_titles leads to improper neutralization of special elements used in a template engine. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-105096	A vulnerability was determined in Omega Solution CoinEx Crypto 2025. This affects an unknown function of the file /customer/ of the component Customer Profile API. Executing a manipulation of the argument ID can lead to authorization bypass. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The product web site does not exist anymore. Maybe the product got retired and/or replaced. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-20532	In apu, there is a possible application crash due to double free. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS11249024; Issue ID: MSV-9168.	6.2	More Details
CVE-2026-103957	Server-side request forgery in the OAuth2 discovery handling in Loom for AWS before 1.7.0 might allow an authenticated remote user to obtain the access token of another user of the deployment and to cause the application to issue requests to arbitrary internal network locations, via a crafted discovery document address supplied when registering a tool server or remote agent configured for delegated authentication. To remediate this issue, users should upgrade to version 1.7.0 or later.	6.2	More Details
CVE-2026-104182	stream-json is a micro-library of stream components for processing JSON and JSONC with a minimal memory footprint. Prior to 3.6.0, the JSONC parser at stream-json/jsonc/parser.js and verifier at stream-json/jsonc/verifier.js restart comment-terminator scanning from the opening slash whenever a block or line comment spans an input chunk, while retaining the accumulated comment buffer. Delivering a large valid comment across many small chunks therefore causes quadratic CPU work and can stall the Node.js event loop. The maintainer characterizes the attack vector as local because the documented JSONC input is locally owned or user-controlled configuration, rather than input intended for the open internet. This JSONC-only scope does not include the plain JSON parser, which advances through and discards consumed string and number data. This issue is fixed in version 3.6.0.	6.2	More Details
CVE-2026-94298	The BuildKit WordPress plugin before 1.0.29 does not properly sanitise and escape data submitted by contributor-level users before storing it and later using it in a SQL query, allowing a Contributor to inject SQL that runs against the database once the resulting content is published and viewed by any unauthenticated visitor.	6.2	More Details
CVE-2026-105114	OpenAM before 16.1.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject script by supplying crafted parameters rendered unencoded on the OAuth2 authorization error page. Attackers can lure victims to a crafted /oauth2/authorize link with repeated parameters to run JavaScript in the OpenAM origin, acting within existing sessions or redirecting to phishing pages.	6.1	More Details
CVE-2026-104465	YesWiki before 4.6.7 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject scripts via the field parameter of the mail handler. Attackers can craft links whose field value breaks out of the ajax-mail-form action attribute to execute JavaScript in victims' browsers.	6.1	More Details
CVE-2026-105117	OpenAM before 16.1.3 contains an email content injection vulnerability that allows unauthenticated attackers to control notification email wording via the forgotPassword and register actions on /json/{realm}/users. Attackers can supply subject and message fields to send phishing mail from the organisation's configured From address, or abuse register as a relay to arbitrary recipients.	6.1	More Details
CVE-2026-93880	The Greenshift - animation and page builder blocks plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via '{{GET:}}' Dynamic Placeholder in all versions up to, and including, 13.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This requires a site administrator to have configured an element block's Custom JS field to include a '{{GET:...}}' placeholder and for that JS to contain the token 'import', which routes the substituted value to the unescaped raw echo branch inside a <script type="module"> tag.	6.1	More Details
CVE-2026-	YesWiki before 4.5.3 contains multiple reflected cross-site scripting vulnerabilities that allow remote attackers to inject JavaScript through unsanitized parameters such as incomingurl, id, file, tags, and	6.1	More

104473	template. Attackers can lure authenticated or unauthenticated users into opening crafted links to hijack sessions and trigger authenticated requests against backend functionality.		Details
CVE-2026-97652	The WP Statistics – Simple, privacy-friendly Google Analytics alternative plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via REQUEST_URI Query-Parameter Key in all versions up to, and including, 14.16.14 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-105116	OpenAM before 16.1.3 contains a latent cross-site scripting defect that places the SAML message, relay state and target URL unencoded into the load-balancer cookie bounce auto-submit page. If reachable with cookieHashRedirectEnabled set, crafted requests could execute script in the OpenAM origin, though an unrelated HTTP 500 failure prevents exploitation in released versions.	6.1	More Details
CVE-2026-103909	The Calculated Fields Form – AI Form Builder for WordPress – Contact, Payment, Quote, Quiz & More plugin for WordPress is vulnerable to Reflected DOM-Based Cross-Site Scripting via the 'arbitrary (whichever names the admin bound via url.<name>)' parameter in all versions up to, and including, 5.5.1.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires the targeted site to host a publicly accessible form in which an administrator has configured at least two fields with url.&name> predefined values that are used together in a concatenation equation — a plausible but not universal configuration.	6.1	More Details
CVE-2026-103888	The WPC Smart Quick View for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'woosq-redirect' parameter in all versions up to, and including, 4.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The WooCommerce "redirect to cart after add to cart" option must be enabled for the filter that reads the woosq-redirect parameter to execute; however, the ?quick-view= auto-open mechanism means no further user interaction beyond loading the crafted URL is required to trigger script execution.	6.1	More Details
CVE-2026-92826	The EWWW Image Optimizer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via REQUEST_URI Parameter Key in all versions up to, and including, 8.7.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Successful exploitation requires that the enable_help option is active, as the vulnerable HelpScout Beacon script block is only emitted when that setting is enabled.	6.1	More Details
CVE-2026-95165	Bacularis 5.4.0 - 6.5.1 is vulnerable to Cross Site Scripting (XSS) in the Organization name field.	6.1	More Details
CVE-2026-85492	The All in One SEO – AI SEO Plugin to Boost SEO Rankings & Traffic (Schema, Local SEO, Sitemap & SEO Insights) plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting via URL Pathname in all versions up to, and including, 5.0.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user visits a crafted URL. Exploitation requires the victim to hold the aioseo_manage_seo capability and to open the SEO Preview panel in the WordPress admin toolbar while visiting a page with a malicious payload embedded in the URL pathname.	6.1	More Details
CVE-2026-92551	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via ppress_billing_address Filename Parameter in all versions up to, and including, 4.17.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The vulnerability is exploitable via any page hosting the ProfilePress Tabbed Widget by supplying a malicious filename for the ppress_billing_address file upload field in a crafted POST request.	6.1	More Details
CVE-2026-92538	The LearnPress – WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Reflected DOM-Based Cross-Site Scripting via the 'orderby' parameter in all versions up to, and including, 4.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'thumb_url' parameter in all versions up to, and including, 1.8.46		

CVE-2026-92974	due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires that the authenticated victim holds the manage_options capability, as the editimage_bwg AJAX action performs a capability check but no nonce verification, meaning the payload can be delivered via a crafted GET request without a CSRF token.	6.1	More Details
CVE-2026-92243	The Ivory Search – WordPress Search Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in all versions up to, and including, 5.5.18 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that the targeted search form has the 'Highlight Search Terms' option enabled by an administrator, and that the malicious search query returns at least one post result.	6.1	More Details
CVE-2026-105124	W (vincent-peugnet/wcms) through 3.18.0 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject scripts via the login user field and visitor comment website field. Attackers can submit failed logins rendered unescaped in the adminlog.php log viewer, or comment URLs echoed into href attributes in editrightbar.php, executing script with administrator or editor privileges.	6.1	More Details
CVE-2026-93896	The WPFront Notification Bar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in versions up to, and including, 3.5.1. This is due to the debug-log output path (write_debug_logs) reflecting the raw value of \$_SERVER['REQUEST_URI'] through vprintf() directly inside a <script> block emitted on wp_footer, without any sanitization or escaping (see the 'Current URL is "%s"' log entry produced by the URL-text display filter in the filter() method). 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 specially crafted link.	6.1	More Details
CVE-2026-104477	Showdown through 2.1.0 contains a cross-site scripting vulnerability in the makehtml link and image subparsers, which fail to escape double quotes in destination URLs placed into href and src attributes. Attackers can craft markdown links or images containing a double quote followed by onerror or onmouseover handlers to execute script when victims view rendered HTML.	6.1	More Details
CVE-2026-104313	The WPC Estimated Delivery Date for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'rule_data' parameter in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-103048	URL redirection to untrusted site ('open redirect') vulnerability in The Wikimedia Foundation Mediawiki - Collection extension allows Fake the Source of Data. This issue affects Mediawiki - Collection extension: before 1.46.1, 1.45.5, 1.43.10.	6.1	More Details
CVE-2026-89047	The Social Media Share Buttons & Social Sharing Icons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the victim to be on a mobile user-agent and to click the WeChat share icon, though once the dialog opens, script execution is automatic and requires no further user interaction.	6.1	More Details
CVE-2026-103051	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - CentralNotice extension allows Stored XSS. This issue affects Mediawiki - CentralNotice extension: before 1.46.1, 1.45.5, 1.43.10.	6.1	More Details
CVE-2026-19902	The Ad Inserter – Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the Referer header in all versions up to, and including, 2.8.18 due to insufficient input sanitization and output escaping on the '{search-query}' dynamic tag. When an ad block's code contains that tag, replace_ai_tags() reads \$_SERVER['HTTP_REFERER'] and tests it with the regex /[\\V](google yahoo bing ask)\\.([a-z\\.]{2,5}[\\V])/i. The leading [\\V] class matches a literal slash, so any referrer merely containing a segment such as '/google.com/' passes as a search-engine referral; the plugin then percent-decodes the referring query with parse_str() and substitutes the resulting 'q' (or 'p') value into the block via preg_replace() with no escaping. This makes it possible for unauthenticated attackers to execute arbitrary JavaScript in the context of the site for any visitor, including a signed-in administrator, by luring them to an attacker-controlled page that frames or links to any ordinary post. Exploitation requires the site to have an ad block whose code uses the '{search-query}' tag with automatic insertion enabled — a documented plugin feature used as intended.	6.1	More Details
CVE-	A flaw was found in oauth-proxy. The application fails to properly validate the destination redirect parameter (`rd`) during post-login redirection. A remote attacker can exploit this vulnerability by		More

2026-83589	enticing a user to follow a specially crafted link, resulting in the user being redirected to an arbitrary external website after authenticating. This open redirect can be leveraged to conduct phishing attacks or credential theft.	6.1	Details
CVE-2026-97318	The Giveaways and Contests by RafflePress WordPress plugin before 1.12.27 does not properly validate a giveaway's parent page URL before saving it and later redirecting visitors to it, allowing unauthenticated attackers to make the site's own giveaway confirmation and referral links redirect visitors to an arbitrary external site.	6.1	More Details
CVE-2026-89427	The Ad Inserter – Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 's' Search Parameter in all versions up to, and including, 2.8.18 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires that a site administrator has configured at least one Ad Inserter block using the {title} or {short-title} placeholder with that block enabled for search pages, which is a standard, documented plugin feature.	6.1	More Details
CVE-2026-100179	The Calculated Fields Form – AI Form Builder for WordPress – Contact, Payment, Quote, Quiz & More plugin for WordPress is vulnerable to Reflected DOM-Based Cross-Site Scripting via the 'x (any URL parameter consumed by the form's calculated equation)' parameter in all versions up to, and including, 5.5.1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires the target site to have a public form configured with a Select2-enabled dropdown whose choices are populated via a calculated equation that pipes a URL parameter through GETURLPARAMETER() into setChoices({texts: [...]}); given that configuration, exploitation requires only a single crafted link.	6.1	More Details
CVE-2026-84925	The Avada Website Builder For WordPress & WooCommerce theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'lang' parameter in all versions up to, and including, 7.16.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The injected value is propagated through Fusion_Multilingual::set_active_language() and concatenated into a URL by Fusion_Settings::get_setting_link() without applying urlencode(), esc_url(), or esc_attr() before being echoed raw into a double-quoted href attribute in the post editor metabox.	6.1	More Details
CVE-2026-103050	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - MassMessage extension allows Stored XSS. This issue affects Mediawiki - MassMessage extension: before 1.46.1, 1.45.5, 1.43.10.	6.1	More Details
CVE-2026-103049	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in The Wikimedia Foundation Mediawiki - Cargo extension allows Reflected XSS. This issue affects Mediawiki - Cargo extension: before 1.46.1.	6.1	More Details
CVE-2026-102459	EasyFlow .NET developed by Digiwin has a Reflected Cross-site Scripting vulnerability. Unauthenticated remote attackers can execute arbitrary JavaScript codes in user's browser through phishing attacks.	6.1	More Details
CVE-2026-47096	AJA HELO Plus firmware before 2.1.7 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers with network access to inject malicious JavaScript by setting an unsanitized eParamID_SystemName value through the /config?action=set web configuration API. Attackers can exploit this flaw when device authentication is disabled to persistently execute arbitrary script in the browser of any administrator who opens the web management interface, enabling theft of stored secrets such as web UI credentials, RTMP stream keys, publish URLs, and NFS/SMB share credentials, as well as hijacking of the authenticated session.	6.1	More Details
CVE-2026-47518	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a secure microcontroller component, where incorrect permission assignment for a critical resource allows an attacker with privileged local access to modify protected memory that should be restricted. A successful exploit of this vulnerability might lead to code execution and escalation of privileges.	6.0	More Details
CVE-2026-104844	PostCSS Selector Parser is a CSS selector parser that integrates with PostCSS but does not require it. Prior to 7.1.6, src/parser.js splitWord() can receive a flat selector as one word token carrying many class or ID indexes because period and hash characters are not tokenizer word delimiters. The uniqs() deduplication and per-index class and ID membership checks repeatedly scan the class and ID index arrays, while a separate Sass-interpolation filtering pass also performs repeated linear scanning. Together, these passes make parsing quadratic in the number of indexes and allow a crafted selector to occupy a synchronous parser thread. The maxNestingDepth guard does not mitigate the issue because the hostile selector can have zero nesting depth. Only consumers that synchronously parse untrusted	5.9	More Details

	selectors in an exposed request path are affected; ordinary build-time parsing of trusted sources is not affected. This issue is fixed in version 7.1.6.		
CVE-2026-103754	A flaw was found in ansible-runner. The unstream_dir() function, which receives and extracts a streamed zip archive on the worker side of the ansible-runner transmit/worker protocol, re-creates symbolic links from archive content without validating the link target and applies chmod() and utime() to an unsanitized filesystem path derived from the archive member name. A crafted archive processed by a worker that consumes attacker-influenced input can create files, create symbolic links, or change permissions outside the intended target directory, which can be leveraged toward code execution.	5.9	More Details
CVE-2026-102110	An endpoint used during initial appliance setup did not require authentication and did not correctly enforce its intended state precondition, so during the initial activation window an unauthenticated network attacker could repeatedly re-trigger the privileged activation process. This could disrupt setup and leave the appliance in an incompletely configured state. The issue is only reachable while an appliance is being activated for the first time and not yet fully configured.	5.9	More Details
CVE-2026-105292	Chaterm before 0.12.1 contains a login cross-site request forgery vulnerability that allows remote attackers to inject login state by sending chaterm:// callbacks without OAuth state validation. Attackers can trigger a crafted callback with attacker-controlled userInfo from a web page, signing the victim into the attacker's account so default data sync uploads saved hosts, passwords, and private keys.	5.9	More Details
CVE-2026-100276	In JetBrains YouTrack before 2026.2.19197 guest users could remove a workflow action's visibility restriction and run the action	5.9	More Details
CVE-2026-103263	Tornado before 6.5.9 contains a path traversal vulnerability in StaticFileHandler that follows symbolic links inside the static root without confirming the resolved target stays within it. When a symlink pointing outside the static directory exists inside it, unauthenticated attackers can request it to read files such as configuration files, private keys, and application secrets accessible to the process user.	5.9	More Details
CVE-2026-55174	UltrafastSecp256k1 is a high-performance, multi-backend secp256k1 engine with reproducible audit evidence, compatibility shims, and profile-based review scopes. Prior to version 4.2.0, UltrafastSecp256k1's ECDSA adaptor pre-signature verification accepts forged adaptor pre-signatures whose "r" value is not cryptographically bound to the adaptor point "T". This issue has been patched in version 4.2.0.	5.9	More Details
CVE-2026-104476	Backdrop CMS before 1.35.1 contains an information disclosure vulnerability that allows unauthenticated attackers to retrieve configuration export archives left on the server after transfer. Attackers can download compressed archives generated by users with configuration export permission to obtain the full site configuration, including sensitive settings.	5.9	More Details
CVE-2026-105690	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, logout clears the browser's auth-token cookie without revoking the corresponding server-side session. A previously captured session token remains usable after the victim logs out and can continue to make authenticated requests with the victim's authority until natural expiration. This issue is fixed in version 2.18.0.	5.9	More Details
CVE-2026-94681	Unauthenticated Denial of Service Attack in WP Store Locator < 3.0.0 versions.	5.9	More Details
CVE-2026-103760	Mooncake transfer engine through 0.3.13.post1 contains a denial of service vulnerability that allows unauthenticated remote attackers to block the handshake daemon by never reading replies. Attackers can send a Metadata request to the handshake RPC port and stall SocketHandShakePlugin's single listener thread in writeFully(), breaking all subsequent handshakes, metadata fetches, notify and probe requests.	5.9	More Details
CVE-2026-100267	In JetBrains YouTrack before 2026.2.19197 reDoS attack was possible via mailbox regex mail-rule filters	5.9	More Details
CVE-2026-102384	Author Cross Site Scripting (XSS) in Supreme Modules Lite <= 2.5.63 versions.	5.9	More Details
CVE-2026-104426	Zebra before 6.1.0 contains an inefficient algorithmic complexity vulnerability in remaining_transaction_value that clones the entire block-level spent-UTXO map per transaction during contextual verification. Attackers can mine or seed the mempool with roughly 26,000 minimal single-input transactions in one block, stalling every validating node for over 52 seconds.	5.9	More Details

CVE-2026-104427	Zebra before 6.1.0 contains an incomplete cleanup vulnerability in the state write task that allows remote unauthenticated peers to stall node synchronization by poisoning parent_error_map. Attackers can deliver a coinbase-malleated block sharing a canonical block's hash before it propagates, causing the next canonical block to be rejected and stalling the node for roughly 2,000 blocks.	5.9	More Details
CVE-2026-13607	The File Uploads Addon for WooCommerce WordPress plugin through 1.7.6 stores customer-uploaded files in a publicly web-accessible uploads directory and the access restriction it generates is ineffective, so an unauthenticated attacker who knows or guesses a file's name can retrieve customer-uploaded files directly, bypassing the File Uploads Addon for WooCommerce WordPress plugin through 1.7.6's authenticated download mechanism.	5.9	More Details
CVE-2026-78371	The File Uploads Addon for WooCommerce WordPress plugin before 1.7.6 does not verify that the person requesting a customer-uploaded file is the customer who uploaded it, allowing unauthenticated attackers who know or guess a file's name to download other customers' uploaded files.	5.9	More Details
CVE-2026-104356	PictShare before version 3.7.1 contains a weak randomness vulnerability where the getRandomString() function uses the non-cryptographic rand() PRNG to generate the delete_code authorization token in src/inc/core.php. Attackers can predict or infer the PRNG state to guess valid delete_code values and perform unauthorized deletion of hosted files without needing to read the code from the info endpoint.	5.9	More Details
CVE-2026-105695	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, assemble-chunks retrieves an upload session using only its session ID, while upload-chunk correctly scopes the lookup to the authenticated profile. An authenticated user who obtains another user's live, completed upload-session UUID can assemble the victim's chunks into the attacker's own file, team font, or project import, disclosing the uploaded bytes and deleting the victim's pending session. This issue is fixed in version 2.18.0.	5.9	More Details
CVE-2026-104442	YesWiki before 4.6.7 contains an unauthenticated server-side request forgery vulnerability that allows remote attackers to make the server fetch arbitrary URLs by supplying a syndication action through the render handler's content parameter. Attackers can target internal hosts and ports, read back fetched feed content in the rendered page, and cause feed enclosures to be downloaded into the files directory.	5.8	More Details
CVE-2026-103243	LightLLM through 1.2.0 fails to validate image_url and audio_url parameters in multimodal endpoints, allowing unauthenticated attackers to perform server-side request forgery. Attackers can supply arbitrary URLs to fetch internal resources, with vision model processing disclosing content or error responses revealing internal network topology.	5.8	More Details
CVE-2026-103763	SiYuan before v3.8.5 contains an information disclosure vulnerability that allows read-only publish readers to learn metadata of publish-excluded documents through the getNotebookInfo endpoint. Attackers, including anonymous visitors when no reader password is set, can query publish-visible notebooks to obtain document count, size and modification timestamps of hidden documents.	5.8	More Details
CVE-2026-105049	Zilliz Attu before 3.0.0 has a Playground feature that does not require authentication for proxying arbitrary HTTP and HTTPS requests to URLs on the public internet.	5.8	More Details
CVE-2026-104872	OpenTelemetry JavaScript Contrib provides instrumentation libraries for collecting telemetry from JavaScript applications. Prior to versions 0.66.0 of @opentelemetry/instrumentation-cassandra-driver, 0.65.0 of @opentelemetry/instrumentation-knex, 0.67.0 of @opentelemetry/instrumentation-mongoose, @opentelemetry/instrumentation-mysql, and @opentelemetry/instrumentation-mysql2, 0.46.0 of @opentelemetry/instrumentation-oracledb, 0.73.0 of @opentelemetry/instrumentation-pg, and 0.40.0 of @opentelemetry/instrumentation-tedious, the packages add the database connection username to every instrumented database operation as the db.user span attribute. The attribute is emitted by default and is not controlled by enhancedDatabaseReporting or another opt-in setting. Configured observability backends therefore receive database account names that may expose service topology, role or environment information, and account naming patterns. This issue is fixed in versions 0.66.0, 0.65.0, 0.67.0, 0.46.0, 0.73.0, and 0.40.0 of the respective packages.	5.8	More Details
CVE-2026-97316	The Broken Link Notifier WordPress plugin before 2.0.0.1 does not re-validate the destination of redirects when checking links, allowing unauthenticated attackers to bypass its internal-address filter and make the server send requests to internal services.	5.8	More Details
CVE-2026-105302	A flaw was found in the User Session Note mapper of the Keycloak identity and access management solution. The issue occurs because the mapper does not validate whether a requested session note contains sensitive internal credentials, such as federated access tokens from external identity providers. This allows a delegated client administrator to leak a user's upstream bearer tokens into the tokens issued to their managed application, potentially leading to unauthorized access to the user's data on external platforms.	5.7	More Details

CVE-2026-103222	A vulnerability was determined in Blosc C-Blosc2 up to 3.3.2. This impacts the function <code>blosclz_decompress</code> of the file <code>blosc/blosclz.c</code> of the component <code>blosclz Decompression</code> . Executing a manipulation can lead to integer overflow. The attack may be launched remotely. A high complexity level is associated with this attack. The exploitability is said to be difficult. Upgrading to version 3.3.3 will fix this issue. This patch is called <code>fe2964d114d97847f56570a0ab2be2c57ccbeedc</code> . The affected component should be upgraded.	5.6	More Details
CVE-2026-103397	OpenSave before 2.4.0-beta.1 fails to validate sender identity in WAN relay requests, allowing unpaired room members to impersonate paired devices by spoofing the <code>RelayMessage From</code> field. Attackers who know the room code can join, read paired peer identifiers from announcements, and send forged requests to access protected sync routes including save data, snapshots, and file operations.	5.6	More Details
CVE-2026-104030	A flaw was found in <code>sssd</code> . This vulnerability allows a local user to cause a Denial of Service (DoS) by submitting a specially crafted passkey authentication token that lacks null terminators. The authentication service reads past the end of the provided memory buffer, causing the process to crash and disrupting authentication services.	5.5	More Details
CVE-2026-97238	Subscriber Cross Site Scripting (XSS) in JetEngine <= 3.8.14.3 versions.	5.5	More Details
CVE-2026-103497	In JetBrains YouTrack before 2026.2.19422 sSRF was possible via the GitHub VCS integration	5.5	More Details
CVE-2026-78413	Velociraptor allows collection of VQL queries packaged into Artifacts from endpoints. These artifacts can be used to do anything and usually run with elevated permissions. To limit access to some dangerous artifact, Velociraptor allows for those to require high permissions like <code>EXECVE</code> to launch. The <code>`Windows.Sysinternals.SysmonLogForward`</code> is a monitoring artifact used to forward <code>sysmon</code> events to the server. The artifact allows the user to specify an arbitrary binary path as a parameter, and did not enforce an additional required permission, allowing users with <code>COLLECT_CLIENT</code> permissions (normally given by the "Investigator" role) to collect it from endpoints and run a different binary program than the installed <code>sysmon</code> binary. To successfully exploit this vulnerability the user must already have access to collect artifacts from the endpoint (i.e. have the <code>COLLECT_CLIENT</code> given typically by the "Investigator" role).	5.5	More Details
CVE-2026-102578	A flaw was found in Moodle. An authenticated attacker with access to the question bank web service can submit unsanitized input directly into database queries, resulting in a SQL (Structured Query Language) injection vulnerability. This issue could allow an attacker to view, alter, or delete sensitive data stored in the underlying database.	5.5	More Details
CVE-2026-28667	In multiple functions of <code>rw_t5t.cc</code> , there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-47492	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where an attacker can cause improper access control. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-58834	In <code>setPermissionGrantState</code> of <code>DevicePolicyManagerService.java</code> , there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-47557	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause a NULL pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-95512	A flaw was found in FreeType, specifically within its CID font loader. A remote attacker could exploit this vulnerability by tricking a user into opening content that embeds or references a specially crafted CID-keyed font. This crafted font can cause repeated allocations and decryptions of subroutine data across multiple font dictionaries, leading to excessive memory and CPU consumption. This can result in a denial of service (DoS) for the application or service processing the font, potentially causing it to hang or terminate.	5.5	More Details
CVE-2026-47581	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where a user could cause improper locking. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where a user could cause uncontrolled resource consumption by exhausting the DRM VMA offset address space. A	5.5	More

47567	successful exploit of this vulnerability might lead to denial of service.		Details
CVE-2026-47566	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an unprivileged user could cause a memory leak in error paths leading to kernel memory exhaustion. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-20543	In Modem, there is a possible information disclosure due to a logic error. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01645293; Issue ID: MSV-6761.	5.5	More Details
CVE-2026-47555	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where a user could cause uninitialized kernel memory to be copied back to userspace. A successful exploit of this vulnerability might lead to information disclosure.	5.5	More Details
CVE-2026-47549	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel module where an unprivileged local user could cause a NULL pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-47534	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause a divide by zero. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-47568	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a user could cause uncontrolled kernel log generation by repeatedly invoking an interface that emits unrate-limited error messages. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-47584	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel module where an attacker with local access could cause a NULL pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-103531	A flaw has been found in OpenSC up to 0.27.1. The impacted element is the function setcos_construct_fci_44 of the file src/libopensc/card-setcos.c. Executing a manipulation of the argument type_attr can lead to stack-based buffer overflow. The attack can be launched remotely. This patch is called ad730304052937c32b4eb489a06835ac6123632c. It is best practice to apply a patch to resolve this issue.	5.5	More Details
CVE-2026-103641	A flaw was found in GEGL. The Radiance HDR loader reads past the end of a memory-mapped image when an uncompressed scanline is shorter than the width declared in the file header. Opening a crafted HDR file crashes the application that uses the loader.	5.5	More Details
CVE-2026-105447	A flaw was found in Quay. When handling build trigger requests, the application incorrectly exposes trigger configuration details containing repository write tokens to global read-only administrative users. An authenticated user with read-only privileges can exploit this flaw by querying the build trigger API to retrieve these delegate tokens. This issue allows a restricted user to bypass read-only limitations and push arbitrary container images to private repositories, leading to privilege escalation.	5.5	More Details
CVE-2026-47603	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode driver where a local user may access another process's GPU channel state due to missing authorization checks. A successful exploit of this vulnerability might lead to information disclosure.	5.5	More Details
CVE-2026-47517	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode driver where a local user may cause a null pointer dereference by submitting a crafted ioctl. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-47604	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode driver where a local user may access another process's GPU channel state due to missing authorization checks. A successful exploit of this vulnerability might lead to information disclosure.	5.5	More Details
CVE-2026-47506	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel-mode color transform path where excessive kernel stack use occurs when evaluating YCbCr420 display emulation. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2026-39444	Authorization Bypass Through User-Controlled Key vulnerability in PublishPress PublishPress Series organize-series allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PublishPress Series: from n/a through 3.1.3.	5.4	More Details
CVE-2026-	A flaw was found in Quay. A cross-site scripting (XSS) vulnerability in the OAuth callback handler allows a remote attacker to execute arbitrary JavaScript code within a user's browser session. By tricking a logged-in user into visiting a specially crafted link, an attacker can exploit improper input sanitization to run client-side scripts in the application context. Successful exploitation could allow the attacker to	5.4	More Details

102295	compromise the user's session, access sensitive registry information, or perform unauthorized actions on their behalf.		
CVE-2026-96450	Contributor Cross Site Scripting (XSS) in pixfort Core < 4.3.3 versions.	5.4	More Details
CVE-2026-103079	Authorization Bypass Through User-Controlled Key vulnerability in Ahmad JS Help Desk js-support-ticket allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JS Help Desk: from n/a through 4.0.0.	5.4	More Details
CVE-2026-94173	Contributor Insecure Direct Object References (IDOR) in Business Directory <= 6.4.27 versions.	5.4	More Details
CVE-2026-90972	The WP Fusion Lite WordPress plugin before 3.48.0 does not perform a capability check on two of its admin AJAX handlers, allowing any authenticated subscriber to read other users' email addresses and to trigger a cross-user CRM re-sync.	5.4	More Details
CVE-2026-62083	Subscriber Other Vulnerability Type in Creator LMS <= 1.2.19 versions.	5.4	More Details
CVE-2026-62081	Contributor Insecure Direct Object References (IDOR) in Flexible PDF Coupons <= 1.14.11 versions.	5.4	More Details
CVE-2026-102399	Unauthenticated Cross Site Request Forgery (CSRF) in Photo Gallery by Supsysitic <= 1.21.0 versions.	5.4	More Details
CVE-2026-104967	Plane is an open-source project management tool. Prior to 1.4.0, BulkDeletelssuesEndpoint and SublssuesEndpoint in apps/api/plane/app/views/issue/ accept body- or URL-supplied issue IDs and operate on them without checking that the IDs belong to the caller's workspace and project. The permission decorator on each endpoint validates only that the caller is a member or administrator of the workspace and project named in the URL. BulkDeletelssuesEndpoint can destroy Cyclelssue and Modulelssue associations belonging to foreign issues. SublssuesEndpoint can re-parent foreign issues under an attacker-selected issue and return the foreign issues' metadata. This issue is fixed in 1.4.0.	5.4	More Details
CVE-2026-13720	An Editor can set file-provisioning metadata (the grafana.app/managedBy, grafana.app/managerId and grafana.app/sourcePath annotations) when creating a dashboard through the dashboard API, because these fields were stored without an authorization check. The dashboard then appears file-provisioned, and administrators can no longer update or delete it through Grafana. The impact is limited to the same organization and no data is exposed.	5.4	More Details
CVE-2026-19954	Net::Whois::Raw versions before 2.99044 for Perl ship a pwhois command-line tool that queries WHOIS for the wrong domain for unicode domain names. pwhois encodes each non-ASCII label directly using Net::IDN::Punycode and prepends xn--. Apart from lowercasing ASCII and Cyrillic letters, it skips the IDNA mapping and normalization steps, so a label with other uppercase letters, or not in NFC, encodes to a different A-label than its IDNA form. For example, a label of U+00C9 followed by "cole" encodes to "xn--cole-pka" rather than "xn--cole-9oa". The Net::Whois::Raw library modules are not affected.	5.4	More Details
CVE-2026-104466	YesWiki before 4.6.7 contains a stored cross-site scripting vulnerability in formatters/wakka.php that allows users who can edit pages or post comments to inject event handlers by placing quotes in markdown image URLs. Attackers can store a crafted markdown image whose src breaks out of the attribute to add an onerror handler, executing JavaScript in viewers' browsers, including administrators.	5.4	More Details
CVE-2026-104181	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.13.3 and 5.8.3, app-based multi-factor authentication management actions do not consistently require confirmation of the current password. An attacker with access to an authenticated user session can set up app-based MFA and obtain recovery codes, or disable app-based MFA and regenerate recovery codes by supplying an existing app code or recovery code, without knowing the account password. Email-based MFA is not affected, and the issue does not independently permit an unauthenticated sign-in, but changing the app-MFA configuration may lock the legitimate user out. This issue is fixed in versions 4.13.3 and 5.8.3.	5.4	More Details
CVE-2026-	YesWiki before 4.6.7 contains a stored cross-site scripting vulnerability in the Bazar FileField, which validates only the upload's file extension and never calls HtmlPurifierService::cleanFile, so SVG files are stored verbatim and served inline as image/svg+xml. Authenticated users can submit entries via POST	5.4	More

104461	/api/entries/{formId} with SVG files containing script that executes in the wiki origin when the file is opened, enabling administrator session or account compromise.		Details
CVE-2026-104453	YesWiki before 4.6.7 contains a cross-site request forgery vulnerability in the admintag action that allows attackers to delete tag associations by luring administrators to crafted GET links. Attackers can supply a wide id range in the delete_tag parameter via top-level navigation, carrying the SameSite=Lax admin cookie, to bulk-delete tag triples.	5.4	More Details
CVE-2026-104452	YesWiki before 4.6.7 contains a cross-site request forgery vulnerability in the filemanager page handler, which deletes page attachments on GET requests without validating a CSRF token. Attackers can lure a logged-in page owner or administrator into a top-level GET navigation with do=del, erase, or emptytrash, deleting or permanently purging the page's attachments.	5.4	More Details
CVE-2026-97243	Subscriber Broken Access Control in AllAble Connector <= 0.13.4 versions.	5.4	More Details
CVE-2026-94486	Next.js is a React framework for building full-stack web applications. From 16.0.0 until 16.3.8, the next dev development server exposes a Model Context Protocol endpoint without reliably restricting cross-site requests. A malicious website visited by a developer can reach the endpoint and read the project's disk location, source code snippets from error reports, route inventory, and development logs. Production deployments do not serve this endpoint. This issue is fixed in version 16.3.8.	5.4	More Details
CVE-2026-104965	Plane is an open-source project management tool. Prior to 1.4.0, the issue-relation endpoint accepts issue UUIDs in the request body without validating that they belong to the caller's workspace. An authenticated user can create relations linking their own issues to issues in any other workspace on the instance, leaking issue metadata through activity events. This issue is fixed in 1.4.0.	5.4	More Details
CVE-2026-104961	Plane is an open-source project management tool. Prior to 1.4.0, WorkspaceOwnerPermission does not require is_active=True when checking whether a user is a workspace owner. A deactivated user can therefore remain authorized as the workspace owner and retain owner-level access. This issue is fixed in 1.4.0.	5.4	More Details
CVE-2026-105131	ezBookkeeping 1.2.0 before 2.0.1 contains a privilege escalation vulnerability that allows attackers holding an API token to obtain a full session token via /api/v1/tokens/refresh.json. Because TokenRefreshHandler never checks token type, attackers can exchange short-lived or IP-restricted API tokens for 30-day normal session tokens that bypass API token expiry and allowlists.	5.4	More Details
CVE-2026-100261	In JetBrains YouTrack before 2026.2.18991 changing article visibility settings was possible without update permission	5.4	More Details
CVE-2026-39721	Missing Authorization vulnerability in Brainstorm Force Starter Templates astra-sites allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Starter Templates: from n/a through 4.7.7.	5.4	More Details
CVE-2026-12241	The Advanced Woo Labels - Product Labels & Badges for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to an improperly secure capability check on the 'save_meta_boxes' function in all versions up to, and including, 2.51. This makes it possible for authenticated attackers, with Contributor-level access and above, to create AWS labels that are rendered without proper escaping. The vulnerability was partially patched in version 2.46.	5.4	More Details
CVE-2026-103539	A weakness has been identified in ZongXR SuperMarket 1.0.0.0. This affects the function startBuy of the file instant-buy/src/main/java/com/supermarket/instantbuy/controller/InstantBuyController.java of the component Instant Buy. Executing a manipulation of the argument Username can lead to missing authentication. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.4	More Details
CVE-2026-103496	In JetBrains YouTrack before 2026.2.19422 iDOR in inbox threads allowed reading other users' notifications	5.4	More Details
CVE-2026-103421	The WPMobile.App - Android and iOS App Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'REQUEST_URI (path segment after /android_json/search/)' parameter in all versions up to, and including, 11.84 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the app's content mode to be configured as 'webview' (i.e., the 'speed' option is not set to '1'), which is a supported and still-shipped	5.4	More Details

	mode, though no longer the default.		
CVE-2026-105396	Heym before v0.0.112 contains a token leakage vulnerability in build_public_base_url() that allows unauthenticated attackers to redirect HITL review links by spoofing Origin or X-Forwarded-Host headers. Attackers can trigger anonymous workflows with forged headers so reviewer notifications point to attacker domains, capturing capability tokens to submit decisions executed with owner credentials.	5.4	More Details
CVE-2026-103590	QloApps through 1.7.0 contains a reflected cross-site scripting vulnerability in the back-office room type editor's length of stay fields. Attackers can induce authenticated administrators to submit crafted POST requests with malicious payloads in restriction_min_los and restriction_max_los parameters, executing arbitrary JavaScript in the victim's administrative session.	5.4	More Details
CVE-2026-103589	QloApps through 1.7.0 contains a reflected cross-site scripting vulnerability in the back-office room type editor that fails to escape room_num, floor, and comment field values in input attributes. Attackers can induce authenticated back-office users to submit crafted POST requests with malicious payloads to execute arbitrary JavaScript in the victim's administrative session.	5.4	More Details
CVE-2026-103281	Ghost (npm package 'ghost') versions from 3.23.0 up to, but not including, 6.23.0 expose API keys to users with low-privilege staff accounts. An authenticated low-privilege staff user can read API keys returned by the Admin API, which are intended to be available only to higher-privileged users.	5.4	More Details
CVE-2026-103678	A flaw was found in tnef. An attacker can exploit this vulnerability by providing a specially crafted file containing uncompressed Rich Text Format (RTF) data. Because the application fails to properly validate input buffer boundaries before copying data in get_rtf_data_from_buf(), reading beyond the allocated memory occurs. This flaw can cause the application to crash, leading to a Denial of Service (DoS), or leak sensitive memory contents into extracted output files.	5.4	More Details
CVE-2026-103588	QloApps through 1.7.0 contains a reflected cross-site scripting vulnerability in the exceptions field of the back-office Transplant a module form. Attackers can craft a malicious link containing JavaScript payload in the exceptions parameter that executes in an authenticated administrator's session when the victim follows the link.	5.4	More Details
CVE-2026-105224	YesWiki before 4.6.7 contains a cross-site scripting vulnerability in the Bazar valeur action that allows page editors to inject script by rendering unescaped HTML fetched from a remote URL. Attackers can point tools/bazar/actions/valeur.php at a controlled server returning BAZ_fiche_titre markup with an img onerror handler, executing script in every viewer's browser.	5.4	More Details
CVE-2026-103587	QloApps through 1.7.0 contains a reflected cross-site scripting vulnerability in the back-office Hotel Reservation System Book Now search, where date_to and id_room_type parameters are copied into template variables without validation. Attackers can craft a malicious link containing JavaScript payload in these parameters that executes in an authenticated administrator's session when the victim follows the link.	5.4	More Details
CVE-2026-100180	The Jeg Kit for Elementor – Powerful Addons for Elementor, Widgets & Templates for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment in all versions up to, and including, 3.2.19 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Immediate persistence without moderator approval is possible when the attacker submits from an email address with at least one previously approved comment, though the widened allowlist bypasses sanitization regardless of approval status.	5.4	More Details
CVE-2026-104479	Shopclass before 6.2.0 contains a stored cross-site scripting vulnerability that allows self-registered non-admin users to inject scripts into item listing descriptions when frontend TinyMCE is enabled. Attackers can submit malicious JavaScript, which ItemActions.php saves without tag stripping, causing it to execute in the site origin for any visitor viewing the listing.	5.4	More Details
CVE-2026-102134	Kiteworks Core did not apply its gateway-level API security controls to every request authenticated through the platform's central authentication service. An authenticated user could reach REST API functionality over a request path on which those controls, including enforcement of signed-out and revoked sessions, were not applied.	5.4	More Details
CVE-2026-104475	IDURAR ERP CRM through 4.1.1 contains a stored cross-site scripting vulnerability that allows authenticated users to inject scripts by uploading unsanitized SVG files. Attackers can upload JavaScript-laden SVGs via the profile update or settings upload endpoints, which execute in victims' browsers when served from the /public route.	5.4	More Details
CVE-2026-	A vulnerability has been found in Gerapy up to 0.9.13. This vulnerability affects the function project_create of the file gerapy/server/core/views.py of the component Project Management. The manipulation of the argument project_name leads to path traversal. Remote exploitation of the attack	5.4	More

105174	is possible. The exploit has been disclosed to the public and may be used. The identifier of the patch is 6e481078cfba6388a67ca2d9792288405019ba3e. Applying a patch is the recommended action to fix this issue.		Details
CVE-2026-101883	OpenClaw Windows Node through 2026.9.4 contains a server-side request forgery vulnerability in the canvas.present capability that bypasses URL risk evaluation enforced by canvas.navigate. Attackers with gateway or agent access can issue canvas.present to make the node's WebView send requests to localhost, private networks, or tailnet services from the user's machine.	5.4	More Details
CVE-2026-62063	Missing Authorization vulnerability in Magepeople inc. WpTravelly tour-booking-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WpTravelly: from n/a through 2.3.1.	5.4	More Details
CVE-2026-105397	LearnPress plugin for WordPress through 4.4.9.1 contains a stored cross-site scripting vulnerability that allows authenticated instructors to inject scripts via quiz question hint and explanation fields. Attackers with the Instructor role can submit unsanitized payloads through the update_question AJAX handler that execute in the session of every student taking the quiz.	5.4	More Details
CVE-2026-101890	The Prime Mover plugin for WordPress before 2.2.1 contains a stored cross-site scripting vulnerability that allows attackers to execute arbitrary JavaScript by injecting an unescaped site_title value in a package's footprint.json file. Attackers can place a crafted package under the prime-mover-export-files directory so that the malicious value renders unescaped in the column_site_title() method of PrimeMoverBackupMenuListTable.php, triggering script execution in an administrator's browser when they view the Prime Mover Packages list table without needing to restore the package.	5.4	More Details
CVE-2026-97299	Unauthenticated Cross Site Request Forgery (CSRF) in Razorpay Payment Links for WooCommerce <= 2.1.5 versions.	5.4	More Details
CVE-2026-97285	Contributor Broken Access Control in The Events Calendar <= 6.17.5 versions.	5.4	More Details
CVE-2026-104893	Plane is an open-source project management tool. Prior to 1.4.0, GET /api/users/api-tokens/ allows an authenticated user to retrieve API-token records, while PATCH /api/users/api-tokens/{token_id}/ allows the user to modify the token's allowed_rate_limit field without server-side validation or a maximum value. A user can raise the limit arbitrarily and bypass intended API rate-limiting controls, enabling high-volume automated requests, backend resource abuse, and possible resource exhaustion. This issue is fixed in 1.4.0.	5.4	More Details
CVE-2026-104955	Plane is an open-source project management tool. Prior to 1.4.0, a Project Member with role 15 can send a PATCH request to the project-member update endpoint at /api/workspaces/{workspace_slug}/projects/{project_id}/members/{member_pk}/ to change another user's project role. The role-update logic blocks only a new role higher than the requester's role, so assigning the equal Member role bypasses the insufficient validation and promotes a Project Guest with role 5 to Member without Project Admin approval. This unauthorized promotion grants the guest the additional project capabilities associated with the Member role and allows a regular member to bypass project governance controls. This issue is fixed in 1.4.0.	5.4	More Details
CVE-2026-105128	LaraDashboard before 1.4.8 contains an open redirect vulnerability that allows remote attackers to redirect users by supplying an unvalidated redirect_url parameter to EmailTemplateController builder and builderEdit. Attackers can send crafted builder links to logged-in users with email template permissions so saving a template navigates them to attacker-controlled phishing sites.	5.4	More Details
CVE-2026-103519	The The WP Ultimate Review plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.4.3. 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 authenticated attackers, with subscriber-level access and above, to execute arbitrary shortcodes. The bypass relies on WordPress's own strip_shortcodes() function unwrapping the [[tag]] double-bracket escape to a bare [tag] that survives wp_insert_post storage and fires when the publicly queryable xs_review post type is rendered through the_content.	5.4	More Details
CVE-2026-105122	OpenAM before 16.1.3 contains a server-side request forgery vulnerability that allows attackers able to register or modify OAuth 2.0 clients to make OpenAM fetch internal resources via an unvalidated jwks_uri. Attackers can trigger unauthenticated fetches through client-authentication and ID-token validation to probe internal hosts, metadata endpoints or local files, or exhaust request threads for denial of service.	5.4	More Details
	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, authenticated users with file-		

CVE-2026-105694	edit permission can upload SVG media whose scripts, event-handler attributes, and foreignObject elements are stored without sanitization and served as image/svg+xml from the Penpot origin. A victim who navigates to the asset URL executes attacker-controlled JavaScript in that origin, allowing requests and data access with the victim's Penpot session authority. This issue is fixed in version 2.18.0.	5.4	More Details
CVE-2026-71297	A flaw was found in the maestro gRPC broker. This vulnerability allows a remote attacker, with a valid client certificate, to bypass authentication. This bypass enables the attacker to subscribe to other consumers' event streams, leading to unauthorized information disclosure, or to publish forged agent status, which can compromise data integrity.	5.4	More Details
CVE-2026-105698	Langflow is a tool for building and deploying AI-powered agents and workflows. From 1.0.0 until 1.10.1, Langflow did not verify flow ownership in the deprecated POST /api/v1/build/{flow_id}/vertices and POST /api/v1/build/{flow_id}/vertices/{vertex_id} handlers. Through version 1.7.1, an unauthenticated caller who knew another user's flow UUID could reach these handlers; from version 1.7.2 through 1.10.0, callers had to authenticate but needed no elevated privileges. Such a caller could cause retrieve_vertices_order to load and cache the private graph, enumerate its vertex identifiers, and use build_vertex to execute selected vertices and receive their results. build_graph_from_db_no_cache performed a primary-key lookup without an owner filter. This could disclose private flow structure, configured values, and selected outputs and could trigger victim-configured side effects and build-history records, although it did not expose the victim's variable-store credentials or permit modification of the stored flow. This issue is fixed in Langflow 1.10.1 and langflow-base 0.10.1.	5.4	More Details
CVE-2026-105692	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the delete-share-link RPC retrieves a caller-selected share-link ID and verifies only that the caller can edit the parent file. It does not verify that the caller created the share link or has owner or administrator authority, allowing any file editor who knows a share-link UUID to delete links created by other users and revoke external reviewers' access. This issue is fixed in version 2.18.0.	5.4	More Details
CVE-2026-103053	AI SOC versions 9.0.0 before 12.0.0 fail to enforce authentication on the response-action API endpoints when AISOC_DEV_MODE is enabled and AISOC_ACTIONS_SERVICE_TOKEN is empty in the default Docker Compose deployment. Unauthenticated attackers can list response-action integrations, submit and approve actions on behalf of arbitrary principals, and dispatch containment actions using vendor credentials.	5.4	More Details
CVE-2026-92924	The Unlimited Elements for Elementor WordPress plugin before 2.0.21 does not check that a request to render widget output comes from a user allowed to make it, allowing users with a role as low as subscriber to have arbitrary WordPress shortcodes executed on the site. Version 2.0.18 removed the subscriber-level access, so from 2.0.18 onward the issue requires a Contributor role or above.	5.4	More Details
CVE-2026-95166	In Bacularis v1.0.0 - 6.5.1 when adding a new pool, the LabelFormat field allows for a Cross Site Scripting (XSS) payload.	5.4	More Details
CVE-2026-85005	The Popup Maker WP WordPress plugin through 1.4.5 does not perform authorization checks on several of its actions and exposes its management page to any logged-in user, allowing users with a low-privileged role such as Subscriber to store display-targeting values that are later invoked as zero-argument PHP callables on public page loads, leading to sensitive information disclosure and denial of service.	5.4	More Details
CVE-2026-78471	The Autoptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Author Name in all versions up to, and including, 3.1.15.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires an administrator to have enabled Autoptimize's 'Lazy-load images?' option, the w3-total-cache/w3-total-cache.php file to be present on disk with the plugin disabled, a class named Minify_HTML to be loaded into scope by another plugin, and the malicious comment to be approved by a moderator before the payload renders.	5.4	More Details
CVE-2026-105421	Missing Authorization vulnerability in Kit Kit (formerly ConvertKit) for WooCommerce convertkit-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kit (formerly ConvertKit) for WooCommerce: from n/a through 2.2.0.	5.3	More Details
CVE-2026-102381	Missing Authorization vulnerability in Ahmad Majestic Support majestic-support allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Majestic Support: from n/a through 1.2.0.	5.3	More Details
CVE-2026-104441	YesWiki before 4.6.7 contains an unauthenticated server-side request forgery vulnerability that allows remote attackers to make the server fetch arbitrary hosts and ports via the {{valeur}} action's url parameter. Attackers can submit the action through the content parameter of handlers/page/render.php to probe internal HTTP services and read back response content matching	5.3	More Details

	fiche markup.		
CVE-2026-102390	Missing Authorization vulnerability in VillaTheme AFFI – Affiliate Marketing for WooCommerce affiliate-marketing-for-woo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AFFI – Affiliate Marketing for WooCommerce: from n/a through 1.0.9.	5.3	More Details
CVE-2026-105030	Kener 4.0.0 before 4.1.6 contains an information disclosure vulnerability that allows unauthenticated attackers to retrieve hidden or inactive monitor data by querying dashboard API handlers lacking visibility filters. Attackers can supply a known or guessed monitor tag to endpoints such as monitor-bar and monitor-latency-chart to obtain names, descriptions, status, uptime history and latency.	5.3	More Details
CVE-2026-103336	Insertion of Sensitive Information Into Sent Data vulnerability in Smackcoders Inc. WP Ultimate CSV Importer wp-ultimate-csv-importer allows Retrieve Embedded Sensitive Data.This issue affects WP Ultimate CSV Importer: from n/a through 9.1.	5.3	More Details
CVE-2026-83560	The New User Approve WordPress plugin before 3.2.10 does not properly verify authentication on a set of integration REST API routes when the integration is unconfigured, allowing unauthenticated attackers to retrieve personal data (id, username, email address and registration date) of registered users.	5.3	More Details
CVE-2026-103340	Missing Authorization vulnerability in Gemini Labs Site Reviews site-reviews allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Site Reviews: from n/a through 8.3.2.	5.3	More Details
CVE-2026-103341	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.20.	5.3	More Details
CVE-2026-90988	The Request a Quote WordPress plugin through 2.5.6 does not perform an authorization check on one of its unauthenticated AJAX handlers, allowing unauthenticated users to read the contact records of quote-request submissions, including records the site has not published.	5.3	More Details
CVE-2026-104440	YesWiki before 4.6.7 contains a blind server-side request forgery vulnerability that allows unauthenticated attackers to make arbitrary server-side requests via the idtypeannounce parameter of /api/entries/bazarlist. Because isValidURL() always returns true, attackers can supply internal URLs fetched by curl in loadURLContent() to probe internal networks and reach internal services or metadata endpoints.	5.3	More Details
CVE-2026-100149	The WPZOOM Connect: AI Chat, Click to Chat, Social Icons & Share Buttons plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.7.3 via the 'x-yamidoo-signature (attacker-obtained via inline_js identify payload)' parameter. This makes it possible for unauthenticated attackers to extract the full customer card — including name, WordPress user ID, order history, order totals, purchased products, payment method labels, and EDD Software Licensing license keys with status and activation counts — for any arbitrary victim email address on the site. Exploitation requires the attacker to register a WooCommerce customer or subscriber-level account with a crafted email address whose local part encodes the target timestamp and victim email, allowing the signature printed into the page HTML by inline_js() to pass verify_request() for an arbitrary victim; both the share_customer_data and identify_logged_in settings are enabled by default, so no non-default configuration is required.	5.3	More Details
CVE-2026-103353	Incorrect Behavior Order vulnerability in WP ManageNinja LLC FluentForm fluentform allows Removing Important Client Functionality.This issue affects FluentForm: from n/a through 6.2.14.	5.3	More Details
CVE-2026-103345	Insertion of Sensitive Information Into Sent Data vulnerability in Shamim Rajani Pie Register pie-register allows Retrieve Embedded Sensitive Data.This issue affects Pie Register: from n/a through 3.8.4.13.	5.3	More Details
CVE-2026-80333	The Solace Extra WordPress plugin before 1.7.2 does not perform any authorization or post-status checks on its front-end preview routes, allowing unauthenticated visitors to read the rendered content of non-published posts and pages of any type that WordPress would otherwise not serve.	5.3	More Details
CVE-2026-103280	Ghost from version 0.8.0 before 6.23.0 contains an information disclosure vulnerability in its setup endpoint: the endpoint responds to unauthenticated requests with the site owner's email address, allowing any remote visitor to obtain it.	5.3	More Details
CVE-2026-103276	Ghost versions before 6.20.0 contain a file extension filtering bypass vulnerability that allows unauthenticated attackers to read theme templates and metadata. Attackers can use URL encoding to bypass extension validation and access sensitive theme files.	5.3	More Details

CVE-2026-103274	Ghost versions 5.3.0 before 6.58.0 fail to properly enforce access controls on comments in private mode. Unauthenticated visitors can read comments that should be restricted, bypassing privacy settings.	5.3	More Details
CVE-2026-103269	Ghost versions 5.3.0 before 6.62.0 contain a missing authorization vulnerability that allows an authenticated site member to read the excerpts of posts they do not have access to (gated content).	5.3	More Details
CVE-2026-86832	The MetForm WordPress plugin before 4.3.1 does not properly restrict access to form submission data, allowing unauthenticated attackers to view submitter information through the REST API.	5.3	More Details
CVE-2026-75824	The User Frontend WordPress plugin before 4.3.12 does not check whether the site allows user registration before creating an account, allowing unauthenticated users to create accounts on sites where registration is disabled. The created account receives the site's default role.	5.3	More Details
CVE-2026-103261	Tornado before 6.5.9 fails to limit the number of query string fields in HTTPServerRequest.__init__, allowing remote attackers to cause event-loop stalling by sending requests with thousands of query parameters. Attackers can send unauthenticated GET requests with unbounded query-string field counts to degrade response times for all clients sharing the same IOLoop.	5.3	More Details
CVE-2026-103245	n8n versions before 1.123.80, from 2.0.0 before 2.39.6, and from 2.40.0 before 2.40.1 fail to verify the x-webflow-signature HMAC in the Webflow Trigger node webhook handler. Unauthenticated attackers can send forged webhook requests with attacker-controlled payloads to trigger workflows and manipulate downstream actions like record creation or API calls.	5.3	More Details
CVE-2026-86789	The Connections Business Directory WordPress plugin through 10.4.67 does not apply its visibility and moderation-status restrictions on certain REST API read endpoints, allowing unauthenticated attackers to retrieve directory entries that are marked private or unlisted, or that are still pending moderation, including entry names, organizations, biographies, internal notes and street addresses. The Connections Business Directory WordPress plugin through 10.4.67 has been closed on WordPress.org and no fixed version is available, so site owners should remove it or restrict unauthenticated access to its REST API routes.	5.3	More Details
CVE-2026-82043	UTMStack before 11.2.16 contains an account enumeration vulnerability that allows unauthenticated attackers to determine registered email addresses by observing differing HTTP responses from the POST /api/account/reset-password/init endpoint. Attackers can submit arbitrary email addresses and distinguish registered accounts, which return 200 OK, from unregistered accounts, which trigger a 500 Internal Server Error with backend error details, enabling targeted phishing or credential attacks.	5.3	More Details
CVE-2026-62058	Insertion of Sensitive Information Into Sent Data vulnerability in WPExperts CF7 Apps contact-form-7-honeypot allows Retrieve Embedded Sensitive Data.This issue affects CF7 Apps: from n/a through 3.7.2.	5.3	More Details
CVE-2026-94543	Next.js is a React framework for building full-stack web applications. From 15.0.0 until 15.5.27 and 16.3.8, self-hosted applications using the Pages Router with statically generated or Incremental Static Regeneration pages can key a response cache entry without sufficiently binding it to the source route. A request can replace one page's cache entry with content from a different route, causing the affected page to serve incorrect content to every visitor until revalidation. Applications deployed on Vercel are not affected. This issue is fixed in versions 15.5.27 and 16.3.8.	5.3	More Details
CVE-2026-103762	SiYuan before v3.8.5 contains a missing authorization vulnerability in the getRefCreateSavePath, getShorthandSavePath, and getDocCreateSavePath endpoints that allows read-only publish visitors to learn unpublished notebook box IDs. Attackers with read-only or anonymous publish access can POST any open notebook ID to receive the global save-box ID and save-path template, revealing a hidden notebook's existence and creation time.	5.3	More Details
CVE-2026-97249	Unauthenticated Bypass Vulnerability in Paid Member Subscriptions <= 3.0.9 versions.	5.3	More Details
CVE-2026-97261	Unauthenticated Sensitive Data Exposure in Notivo <= 1.4.2 versions.	5.3	More Details
CVE-2026-97275	Improper Validation of Specified Quantity in Input vulnerability in VillaTheme BuildKit – Product Builder for WooCommerce – Custom PC Builder woo-product-builder allows Input Data Manipulation.This issue affects BuildKit – Product Builder for WooCommerce – Custom PC Builder: from n/a through 1.0.28.	5.3	More Details

CVE-2026-79768	Path equivalence: '/./' (single dot directory) vulnerability in Apache HTTP Server's mod_userdir module when configured with absolute non-wildcard UserDir directive (the 2nd form in https://httpd.apache.org/docs/2.4/mod/mod_userdir.html#userdir) This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	5.3	More Details
CVE-2026-97282	Unauthenticated Insecure Direct Object References (IDOR) in Review Schema <= 3.1.0 versions.	5.3	More Details
CVE-2026-67171	HCL BigFix Service Management is affected by an Information Disclosure vulnerability because an exposed API endpoint exposes sensitive internal database information. This information could enable an attacker to facilitate targeted database attacks.	5.3	More Details
CVE-2026-58415	Internal state files accessible to external parties in mod_dav_fs in Apache Software Foundation Apache HTTP Server before 2.4.69 on all platforms allows a remote client to read WebDAV dead properties of resources it cannot author via a GET request for the .DAV state directory This issue affects Apache HTTP Server: from 2.4.0 through 2.4.68.	5.3	More Details
CVE-2026-94485	Next.js is a React framework for building full-stack web applications. From 16.0.0 until 16.3.8, the `next dev` development server exposes a Model Context Protocol endpoint without reliably restricting cross-site requests. A malicious website visited by a developer can reach the endpoint and read the project's disk location, source code snippets from error reports, route inventory, and development logs. Production deployments do not serve this endpoint. This issue is fixed in version 16.3.8.	5.3	More Details
CVE-2026-104956	Plane is an open-source project management tool. Prior to 1.4.0, the unauthenticated public issues endpoint accepts group_by and sub_group_by query parameters and passes them without an allowlist to grouped paginators, where they are used as ORM field names by F(field), .values(field), .order_by(field), and Window partition_by operations. An anonymous attacker can supply arbitrary field paths that trigger an unhandled FieldError or KeyError and an HTTP 500 response, or force the ORM to resolve __-separated relational paths as a blind traversal oracle. This is the same field-name injection class addressed by earlier order_by sanitization, but that remediation left group_by and sub_group_by unvalidated. The issue does not directly disclose column values because issue_group_values() returns an empty list for unknown fields, the result projection uses a fixed required_fields list, and the subgrouped path raises KeyError before serialization. This issue is fixed in 1.4.0.	5.3	More Details
CVE-2026-62061	Authorization Bypass Through User-Controlled Key vulnerability in Metagauss ProfileGrid profilegrid-user-profiles-groups-and-communities allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ProfileGrid: from n/a through 6.0.0.2.	5.3	More Details
CVE-2026-94274	The YayReviews WordPress plugin before 1.4.1 does not restrict access to an API route that returns individual customer review records, including reviews still pending moderation, allowing unauthenticated attackers to harvest reviewers' email addresses and other non-public review content.	5.3	More Details
CVE-2026-93580	The InPost PL WordPress plugin before 1.9.8 does not verify the authenticity of incoming shipment webhook requests, relying only on a non-secret identifier and an IP check that is not enforced, allowing unauthenticated attackers who know a target order's parcel tracking number to forge its shipment status and prematurely mark the order completed.	5.3	More Details
CVE-2026-97302	Unauthenticated Sensitive Data Exposure in MPG <= 4.2.3 versions.	5.3	More Details
CVE-2026-67106	HCL BigFix Service Management is affected by an Information Disclosure vulnerability because two exposed API endpoints return sensitive data. This information could enable an attacker to launch further, more serious attacks.	5.3	More Details
CVE-2026-67104	HCL BigFix Service Management is affected by an Information Disclosure vulnerability, which could allow an unauthenticated attacker to analyze publicly accessible JavaScript files, enabling the discovery of hidden administrative API endpoints for further targeted exploitation.	5.3	More Details
CVE-2026-103347	Unauthenticated Bypass Vulnerability in hCaptcha for WP <= 5.3.0 versions.	5.3	More Details
CVE-2026-104874	Multidict is an implementation of a multidict data structure. From 6.7.0 until 6.9.1, the C extension's items-view reflected union operation, operand d.items(), in multidict_itemsview_or2_impl and subtraction operation, d.items() - operand, in multidict_itemsview_sub1_impl fail to release new key-identity and value references returned for each operand element. Applications that perform these operations over attacker-influenced sequences can leak two strong references per element, and garbage collection cannot reclaim them, so repeated operations can cause unbounded process memory	5.3	More Details

	growth and denial of service. Forward union, intersection, non-tuple operand elements, and pure-Python builds are not affected by this reference leak. This issue is fixed in version 6.9.1.		
CVE-2026-105073	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Arraytics WP Event Solution wp-event-solution allows Retrieve Embedded Sensitive Data.This issue affects WP Event Solution: from n/a through 4.1.25.	5.3	More Details
CVE-2026-103004	Next.js versions from 16.3.0 to 16.3.7 warm `use cache` handlers using `next/root-params` and can leak their return value to pages with different root params. With Cache Components enabled (cacheComponents: true), a 'use cache' function that calls another 'use cache' function that reads a root param can be keyed incorrectly when the inner call is served from an existing entry: the enclosing function's cache key then omits that root param. The enclosing entry is written once and reused for all root param values, so a response for one root param value can serve content produced for a different value — whether the page is prerendered at build time or at runtime, or rendered dynamically. Shared cache headers let downstream caches redistribute the content further. What values are leaked cannot be attacker controlled. Which value's content is served depends only on which invocation wrote the entry first. This has been patched in 16.3.8.	5.3	More Details
CVE-2026-92437	The Mailchimp for WooCommerce WordPress plugin before 6.3 does not require authentication, a nonce or an ownership check before it acts on a customer's abandoned-cart record identified from request-supplied data, allowing an unauthenticated attacker to modify or delete another customer's stored cart.	5.3	More Details
CVE-2026-94669	Missing Authorization vulnerability in WP ManageNinja LLC Fluent Forms Pro Add On Pack fluentformpro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent Forms Pro Add On Pack: from n/a through 6.2.13.	5.3	More Details
CVE-2026-94405	Authorization Bypass Through User-Controlled Key vulnerability in Shahjada Download Manager allows Retrieve Embedded Sensitive Data. This issue affects Download Manager: from n/a through 3.3.71.	5.3	More Details
CVE-2026-105693	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the unauthenticated get-view-only-bundle RPC returns every share-link row for a file even when the caller authenticated with only one scoped share link. A holder of a restrictive link can obtain other links' secret IDs, page scopes, comment permissions, and inspection permissions, then replay a more permissive token to access page data that was not included in the original share. This issue is fixed in version 2.18.0.	5.3	More Details
CVE-2026-105161	A flaw has been found in invariant-systems-ai aiir up to 1.7.0. The affected element is an unknown function of the component Policy Gate Handler. Executing a manipulation can lead to improper verification of cryptographic signature. The attack can be executed remotely. It is advisable to upgrade the affected component. The GitHub repository of this project is not available anymore. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-105163	A vulnerability was detected in crossplane crossplane-runtime up to 2.2.2/2.3.2. This vulnerability affects the function Get of the file pkg/xpkg/client.go of the component ImageConfig. The manipulation results in time-of-check time-of-use. The attack may be launched remotely. Upgrading to version 2.2.3, 2.3.3 and 2.4.0-rc.1 is able to resolve this issue. The patch is identified as bee99c6cd6ca81878acca2940a2f0a02169fc208. You should upgrade the affected component.	5.3	More Details
CVE-2026-102144	A resource exhaustion vulnerability in Kiteworks Email Protection Gateway allowed an unauthenticated remote attacker to repeatedly trigger a comparatively expensive server-side operation, causing a partial denial of service.	5.3	More Details
CVE-2026-90952	The WP Edit Password Protected WordPress plugin before 2.0.7 does not enforce its site-wide access restriction on the WordPress REST API, allowing unauthenticated users to read the content of published posts and pages that the site's access mode was configured to hide.	5.3	More Details
CVE-2026-20525	In Modem, there is a possible system crash due to improper input validation. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01870473 / MOLY00814393; Issue ID: MSV-9041.	5.3	More Details
CVE-2026-20527	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01864925 / MOLY01210562; Issue ID: MSV-8303.	5.3	More Details
CVE-2026-104397	Missing Authorization vulnerability in Jeroen Peters Name Directory name-directory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Name Directory: from n/a through 1.34.2.	5.3	More Details

CVE-2026-103476	yii2-starter-kit through 4.2.0 fails to validate article publication status in the attachment-download endpoint, allowing unauthenticated attackers to download files from draft articles. Attackers can enumerate sequential attachment identifiers to retrieve files from unpublished articles without authentication or authorization checks.	5.3	More Details
CVE-2026-104388	Missing Authorization vulnerability in Blubrry Podcasting PowerPress Podcasting powerpress allows Retrieve Embedded Sensitive Data.This issue affects PowerPress Podcasting: from n/a through 11.17.9.	5.3	More Details
CVE-2026-20534	In Modem, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01797547; Issue ID: MSV-9155.	5.3	More Details
CVE-2026-103399	A flaw was found in SoupServer (libsoup). When an HTTP/1.x client sends a request with Expect: 100-continue and a request body, and SoupServer returns an early final (non-1xx) response before the body is read, the server neither drains the declared body bytes nor closes the connection. On a keep-alive connection, those leftover bytes are interpreted as a subsequent HTTP request. A remote, unauthenticated attacker can place a complete HTTP request in the body and cause SoupServer to process that smuggled request, leading to unintended request handling.	5.3	More Details
CVE-2026-20538	In Modem, there is a possible out of bounds read due to a missing permission check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01774038; Issue ID: MSV-8914.	5.3	More Details
CVE-2026-20539	In Modem, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01774038; Issue ID: MSV-8913.	5.3	More Details
CVE-2026-20540	In Modem, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01774038; Issue ID: MSV-8912.	5.3	More Details
CVE-2026-20541	In Modem, there is a possible out of bounds read due to a missing permission check. This could lead to remote denial of service, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01774038; Issue ID: MSV-8911.	5.3	More Details
CVE-2026-90987	The Easy PayPal & Stripe Buy Now Button WordPress plugin before 2.0.6 does not derive the payment amount on the server, taking it from a client-supplied field, so an unauthenticated attacker sets an arbitrary lower price for a purchase.	5.3	More Details
CVE-2026-103351	Improper Validation of Specified Quantity in Input vulnerability in Magepeople inc. Taxi Booking Manager for WooCommerce ecab-taxi-booking-manager allows Input Data Manipulation.This issue affects Taxi Booking Manager for WooCommerce: from n/a through 2.1.1.	5.3	More Details
CVE-2026-91020	The WebToffee Gift Cards for WooCommerce WordPress plugin before 1.3.1 does not validate a user-supplied gift card amount server-side before using it as the cart-item price and store-credit coupon value, allowing unauthenticated users to submit an arbitrary or negative amount, bypassing the configured denominations and manipulating the order total to obtain products without paying.	5.3	More Details
CVE-2026-103241	A flaw has been found in vllm-project vLLM up to 0.26.0. This vulnerability affects unknown code of the file rust/src/parser/src/unified/gemma4.rs of the component Gemma4UnifiedParser. Executing a manipulation can lead to denial of service. The attack may be launched remotely. The exploit has been published and may be used. Upgrading to version 0.29.1rc0 is able to resolve this issue. This patch is called 3439bad37e68ba9755a46f4f6b44a4aeaf1f60a9. Upgrading the affected component is advised.	5.3	More Details
CVE-2026-94432	The Appointment Booking Plugin – LatePoint Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 5.7.1 via the OsPaypalConnectController::create_order_for_transaction() action registered as a public (unauthenticated) route through wp_ajax_nopriv_latepoint_route_call. The handler loads an OsInvoiceModel by a sequential integer 'invoice_id' with no access-key/UUID or ownership check (the sibling Stripe and Razorpay handlers require a 128-bit access-key UUID via OsInvoicesHelper::get_invoice_by_key), and then calls OsTransactionIntentHelper::create_or_update_transaction_intent() which persists a transaction intent tied to the target invoice's customer_id, order_id and charge_amount and regenerates its intent_key before the PayPal-configured guard is reached. This makes it possible for unauthenticated attackers to	5.3	More Details

	enumerate invoices belonging to arbitrary customers, create unauthorized transaction-intent rows linked to another customer's data, and overwrite the intent_key of any in-flight NEW-status transaction intent — invalidating the intent_key that legitimate Stripe/Razorpay flows are waiting on and breaking payment webhooks for those customers.		
CVE-2026-84169	The UPI QR Code Payment Gateway WordPress plugin through 1.4.3 does not verify that a payment-confirmation request actually belongs to the order and customer it claims to confirm, allowing unauthenticated attackers to mark an arbitrary order as paid without making any payment.	5.3	More Details
CVE-2026-80337	Missing Authorization vulnerability in HAVELSAN Inc. Sef - AI Chatbot Platform allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Sef - AI Chatbot Platform: before 2.1. NOTE: The vendor was contacted and it was learned that the product is not supported.	5.3	More Details
CVE-2026-103532	A vulnerability has been found in immich-app Immich up to 2.7.5. This affects the function checkSharedLinkAccess of the file server/src/utls/access.ts of the component Shared Link Preview Handler. The manipulation of the argument Password leads to improper authorization. The attack may be initiated remotely. The reported GitHub issue was closed with the label "duplicate".	5.3	More Details
CVE-2026-103684	Missing Authorization vulnerability in Arraytics WP Event Solution wp-event-solution allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Event Solution: from n/a through 4.1.25.	5.3	More Details
CVE-2026-105055	Missing Authorization vulnerability in WP Mailster WP Mailster wp-mailster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Mailster: from n/a through 1.9.0.0.	5.3	More Details
CVE-2026-11601	The WPCafe – Restaurant Menu, Online Food Ordering & Table Booking System plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.0.19. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to read, create, update, clone, and delete email notification flows, including overwriting the default reservation confirmation, cancellation, and admin alert emails with attacker-controlled content sent from the site's legitimate address, or destroying reservation notification flows entirely. The vulnerable endpoints are active by default on every WPCafe installation without any configuration requirement, as the Email_Automation_Service_Provider::is_enable() method unconditionally returns true and the plugin ships with five pre-configured default email flows upon activation.	5.3	More Details
CVE-2026-12542	A flaw was found in Foreman. The foreman-tail utility is vulnerable to OS command injection due to the unsafe use of the eval command. The script takes user-supplied arguments and incorporates them directly into a string that is then executed by eval to expand file paths. Because the input is not sanitized or quoted, a local attacker can inject shell metacharacters (e.g., ;, &,) to execute arbitrary system commands.	5.3	More Details
CVE-2026-97317	The Giveaways and Contests by RafflePress WordPress plugin before 1.12.27 does not remove the reCAPTCHA secret key from the giveaway settings it embeds in public giveaway pages, allowing unauthenticated visitors to retrieve the secret key of any active giveaway that has reCAPTCHA configured.	5.3	More Details
CVE-2026-13413	The CMP – Coming Soon & Maintenance WordPress plugin before 4.1.20 does not correctly restrict access to the site while maintenance/coming-soon mode is enabled, allowing unauthenticated visitors to bypass the coming-soon page and reach the otherwise hidden site, including hidden published pages, by shaping the request so it is mistaken for a login request.	5.3	More Details
CVE-2026-86556	There is an information disclosure vulnerability in ZTE U30 Air. Due to improper permission control, attackers can exploit the vulnerability to obtain relevant information.	5.3	More Details
CVE-2026-97071	Incorrect Calculation vulnerability in VillaTheme CURCY woo-multi-currency allows Integer Attacks.This issue affects CURCY: from n/a through 2.2.17.	5.3	More Details
CVE-2026-105112	Nezha from 1.8.0 before 2.3.13 contains a lock-order inversion in UpdateGroup and DeleteGroup that allows authenticated non-admin users to deadlock the alerting subsystem. Attackers can concurrently call the notification-group and batch-delete endpoints with oversized id lists to widen the race and close an ABBA cycle, permanently killing alert delivery until restart.	5.3	More Details
CVE-2026-96200	The Payments for Hubtel WordPress plugin before 1.0.2 does not verify that payment notifications received by its payment callback come from the payment provider, allowing unauthenticated attackers to mark arbitrary orders as paid without payment.	5.3	More Details

CVE-2026-96173	The Payments for Hubtel WordPress plugin before 1.0.2 does not verify that the requester is authorized to view an order before redirecting a public payment-callback request, allowing unauthenticated attackers to obtain the order key of an arbitrary order and view its contents.	5.3	More Details
CVE-2026-105127	LaraDashboard 1.4.2 before 1.4.8 applies advanced email validation to unauthenticated forgot-password and reset-password requests, triggering DNS lookups and paid AbstractAPI verification calls. Unauthenticated attackers can submit arbitrary addresses to exhaust the verification quota, making validation fail open for all public forms, and probe domain resolution.	5.3	More Details
CVE-2026-92548	The WP Popular Posts plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.4.2 via the 'context' parameter. This makes it possible for unauthenticated attackers to extract sensitive edit-context fields — including raw title, raw content body, password, meta, status, and guid — from non-public post objects such as wp_block synced patterns that WordPress core itself refuses to expose to unauthenticated callers. This is possible because the plugin's REST route is registered with a permission_callback of __return_true and passes the caller-supplied context parameter (e.g., context=edit) directly to WP_REST_Posts_Controller::prepare_item_for_response() without invoking get_item_permissions_check() or check_read_permission(), while the underlying query accepts an arbitrary post_type value without enforcing public or show_in_rest visibility flags.	5.3	More Details
CVE-2026-100260	In JetBrains YouTrack before 2026.2.18991 mailbox integration allowed authentication after a password reset	5.3	More Details
CVE-2026-104118	The Razorpay for WooCommerce WordPress plugin before 4.8.8 does not perform ownership or authorization checks on a REST API route used during checkout, allowing unauthenticated attackers to modify the shipping information stored on arbitrary orders.	5.3	More Details
CVE-2026-104403	Authorization Bypass Through User-Controlled Key vulnerability in ThimPress LearnPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects LearnPress: from n/a through 4.4.9.	5.3	More Details
CVE-2026-105068	Insertion of Sensitive Information Into Sent Data vulnerability in Pixelite Events Manager events-manager allows Retrieve Embedded Sensitive Data.This issue affects Events Manager: from n/a through 7.4.5.	5.3	More Details
CVE-2026-97332	The User Private Files WordPress plugin before 2.2.0 does not properly protect its stored private files on multisite installations, where the rewrite rule it relies on to route file requests through its access check is never reached, allowing unauthenticated users to retrieve other users' private files directly.	5.3	More Details
CVE-2026-105144	A flaw has been found in Drogon up to 1.9.13-1/10.0-beta.3 on Windows. Affected is the function StaticFileRouter::route of the file lib/src/StaticFileRouter.cc of the component Static File Router. Executing a manipulation can lead to path traversal. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-105145	A vulnerability has been found in Weaviate Verba up to 2.1.3. Affected by this vulnerability is the function get_environment of the file goldenverba/components/util.py of the component generate_stream Endpoint. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-102845	A security vulnerability has been detected in gedelumbung HospitalManagement up to c2d45543789a3887067d3915f69d44cfc2cf76a8. This issue affects the function error_reporting of the file index.php of the component HTTP Response. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-92537	The Newsletter - Send awesome emails from WordPress plugin for WordPress is vulnerable to Insufficiently Protected Credentials in all versions up to, and including, 9.3.9 The plugin's public click-tracking REST route `/tnp/l/` is registered with `permission_callback => '__return_true'` and, upon receiving a valid keyed-MD5 signature, calls `set_user_cookie()`, which emits a `Set-Cookie: newsletter=<id>-<raw_token>` response header to the requester because the subscriber object loaded via `get_user()` lacks the `_trusted` property, causing `get_user_key()` to return the raw token column value instead of its MD5-masked variant. This makes it possible for unauthenticated attackers who obtain any signed click-tracking URL for a target subscriber to receive that subscriber's permanent raw authentication cookie, which they can then use to export the subscriber's full PII record via the	5.3	More Details

	JSON profile-export endpoint (`?na=px`), rewrite the subscriber's stored profile (`?na=ps`), and silently unsubscribe the subscriber via the RFC-8058 one-click endpoint (`?na=ocu`), none of which require a nonce, password, or email challenge. Signed tracking URLs are embedded in every external link of every newsletter delivered to a subscriber, carry no timestamp, and never expire until the site's relink key rotates, meaning that any party who observes such a URL — through a forwarded email, a shared inbox, a mail-gateway log, or Referer headers on the redirect target, which has no Referrer-Policy set — can replay it indefinitely to obtain the victim's credential.		
CVE-2026-105205	SiYuan before 3.8.5 contains an information disclosure vulnerability that allows publish-mode readers to learn backlink block IDs and reference counts from password-protected and publish-disabled documents by querying a published document. Attackers can send POST requests to /api/block/getDocInfo or getDocsInfo for a published document ID to obtain refIDs and refCount of hidden referencing blocks, bypassing the publish confidentiality boundary.	5.3	More Details
CVE-2026-81740	The Paytm Payment Gateway WordPress plugin before 2.8.9 does not verify that payment callbacks genuinely originate from the payment provider when its secret key has not been configured, which is its state immediately after activation, allowing unauthenticated attackers to change the status of arbitrary orders, including marking unpaid orders as paid and reducing stock.	5.3	More Details
CVE-2026-12392	An information exposure vulnerability in Canonical MAAS prior to versions 3.4.10, 3.5.14, 3.6.5, 3.7.3, and 3.8.0 allows an unauthenticated attacker to retrieve the RPC secret in plaintext via the vendor data metadata endpoint. If a target machine was deployed with the 'register as rack' option enabled, an attacker who obtains or infers the machine's system ID can query the preseed/metadata server to leak the secret.	5.3	More Details
CVE-2026-11795	Observable discrepancy vulnerability in Softtr Informatics Trading Limited Company E-Commerce Pack allows Account Footprinting. This issue affects E-Commerce Pack: through 2026-10-02. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-94673	Unauthenticated Insecure Direct Object References (IDOR) in Simply Schedule Appointments <= 1.6.12.31 versions.	5.3	More Details
CVE-2026-102668	The Joyland AI app accepts any TLS certificates from any server without validation.	5.3	More Details
CVE-2026-97066	Unauthenticated Insecure Direct Object References (IDOR) in GiveWP <= 4.16.9 versions.	5.3	More Details
CVE-2026-102669	Joyland AI app does not verify hostnames, allowing a malicious host to connect or intercept chat messages.	5.3	More Details
CVE-2026-104432	Zebra before 6.3.0 contains an improper exceptional condition check in ChainSync::obtain_tips that discards valid one-hash FindBlocks responses, falsely reporting close-to-tip status. Peers returning only the next block hash cause a zero-length sync sample, making the /ready endpoint return 200 OK while the node remains behind the tip.	5.3	More Details
CVE-2026-104455	YesWiki before 4.6.7 contains an access control bypass vulnerability that allows unauthenticated attackers to read restricted page content via the recentchangesrssplus RSS action. Attackers can request the xml method of a page hosting the action to retrieve 500-character body excerpts of every latest page, including read-restricted drafts and notes.	5.3	More Details
CVE-2026-104638	A security vulnerability has been detected in onetwothreeneth HospitalManagementSystem up to 9ef91ed6007314b6473110ed699dff76d158f61d. The impacted element is an unknown function of the file php/sessions.php. The manipulation of the argument ID leads to improper authentication. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-104454	YesWiki before 4.6.7 contains an algorithmic-complexity denial of service in the wakka.php formatter due to an O(n^2) markdown-link regex. Unauthenticated attackers can submit a small crafted body of bracket characters to the page-edit preview endpoint to pin PHP-FPM workers and saturate the pool.	5.3	More Details
CVE-2026-	The Course Booking System WordPress plugin before 7.0.9 does not restrict access to its booking export, allowing unauthenticated users to download the name, email address and billing address of	5.3	More Details

96886	every customer who has booked a course.		
CVE-2026-32584	Insertion of Sensitive Information Into Sent Data vulnerability in Chiranjit Hazarika Smart One Click Setup – Complete Demo Import & Export smart-one-click-setup allows Retrieve Embedded Sensitive Data.This issue affects Smart One Click Setup – Complete Demo Import & Export: from n/a through 1.4.3.	5.3	More Details
CVE-2026-104002	A fail-open error handling issue within the data masking utility of Powertools for AWS Lambda (Python) might allow actors to read sensitive field values that the application intended to mask. To remediate this issue, users should upgrade to version 3.35.0.	5.3	More Details
CVE-2026-104058	Podgrab contains a missing authentication vulnerability in which the /ws WebSocket route is registered on the root gin engine instead of the BasicAuth-protected router group, allowing unauthenticated network clients to connect even when PASSWORD is configured. Attackers can join the allConnections set, capture PlayerExists broadcasts containing client-supplied player identifiers, and replay them in a RegisterPlayer message to hijack queue payloads intended for authenticated users, exposing episode IDs, titles, and server-side file paths while potentially disrupting legitimate playback.	5.3	More Details
CVE-2026-102671	The Joyland AI app accepts invalid SSL certificates in the invisible advertisement WebView by default.	5.3	More Details
CVE-2026-104429	Zebra (zebrad) 5.0.0 before 6.0.0-rc.0 does not apply its per-peer mempool admission cap to transactions received as direct P2P tx messages, because these are queued without the sending peer recorded as their source. A remote inbound peer can push many unique transactions to occupy a disproportionate share of mempool admission slots, crowding out honest peers' transaction relay.	5.3	More Details
CVE-2026-104438	YesWiki before 4.6.7 contains a missing authorization vulnerability in the listpagestag and includepages actions of the tags tool, which enumerate pages without applying read-ACL filtering. Unauthenticated or unprivileged attackers can embed these actions with a chosen tag or page name to disclose the names and body-derived titles of ACL-restricted pages.	5.3	More Details
CVE-2026-104428	The getblock RPC method in zebra-rpc before 11.0.0, used by the Zcash Foundation's Zebra node, panics on verbosity 2 for a side-chain block because the block's -1 confirmations sentinel is converted to u32 with .expect(), aborting the process. Remote unauthenticated attackers, directly or through lightwalletd, can repeat this call to keep the node in a crash loop.	5.3	More Details
CVE-2026-100508	Unauthenticated Denial of Service Attack in Two Factor <= 0.16.0 versions.	5.3	More Details
CVE-2026-104425	ZcashFoundation Zebra before 6.1.0 contains a resource exhaustion vulnerability that allows unauthenticated peers to degrade block processing by pushing transactions with invalid Orchard proofs without being misbehavior-scored. Attackers can repeatedly push invalid proofs into the shared halo2 batch verifier, forcing honest block proofs onto the slow individual-verification path and slowing block processing roughly sevenfold.	5.3	More Details
CVE-2026-104439	YesWiki before 4.6.7 contains a user enumeration vulnerability in LostPasswordAction.php that allows unauthenticated attackers to confirm registered email addresses through differing responses. Attackers can submit emails to the MotDePassePerdu recovery page without rate limiting to identify valid accounts for targeted phishing or password-spraying.	5.3	More Details
CVE-2026-86778	Observable response discrepancy vulnerability in Maksisoft Technology, IT, and Software Industry and Trade Inc. Maksisoft Gym allows Account Footprinting. This issue affects Maksisoft Gym: from 0.5.10 before 0.5.11.	5.3	More Details
CVE-2026-104420	Zebra before 6.3.0 contains a protection mechanism failure that allows unauthenticated peers to evade misbehavior scoring by supplying invalid gossiped blocks. The inbound cleanup step wrongly downcasts RouterError to VerifyBlockError and discards the score, so attackers can repeatedly force block download and Equihash verification without being banned.	5.3	More Details
CVE-2026-97078	Unauthenticated Insecure Direct Object References (IDOR) in Client Invoicing by Sprout Invoices <= 20.8.17 versions.	5.3	More Details
CVE-2026-104421	Zebra before 6.2.1 contains an incomplete cleanup vulnerability that allows unauthenticated peers to block downloading of valid blocks by leaving rejected hashes in SentHashes. Attackers can send a contextually invalid block sharing an honest block's header hash, causing Request::KnownBlock to skip the honest block and keep nodes behind the tip.	5.3	More Details

CVE-2026-5782	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in MRV Technology Foreign Trade Ltd. Co. TurkHotspot allows Reflected XSS. This issue affects TurkHotspot: through 2026-10-02. NOTE: The vendor was contacted and it was learned that the product is not supported.	5.2	More Details
CVE-2026-104183	stream-json is a micro-library of stream components for processing JSON and JSONC with a minimal memory footprint. Prior to 3.6.0, Assembler materializes object properties with plain assignment, so an input key named __proto__ invokes the inherited setter and causes parsed object prototype replacement instead of creating an own data property. Applications that make authorization or feature decisions from inherited values can therefore consume attacker-controlled properties, and a null prototype can disrupt code that expects Object.prototype methods. The researcher treats parsing untrusted JSON as part of the project contract, while the maintainer states that documented inputs are locally owned dumps, exports, or logs and characterizes the attack vector as local. The global Object.prototype is not polluted. This issue is fixed in version 3.6.0.	5.1	More Details
CVE-2026-104470	YesWiki before 4.6.7 contains a server-side request forgery vulnerability that allows page editors to make the server fetch arbitrary URLs via the url parameter of the Bazar valeur action. Attackers can embed the action with a champ parameter in wiki markup to reach loopback or internal services and partially read responses rendered into the page.	5.0	More Details
CVE-2026-82040	UTMStack before 11.2.16 contains a server-side request forgery vulnerability in IdentityProviderService.validateMetadataUrl() that allows authenticated attackers to make the server send requests to arbitrary internal or cloud metadata hosts by supplying a malicious metadata URL to the identity-providers endpoint. Attackers can exploit the POST/PUT /api/identity-providers endpoint with no validation of target host, IP, or scheme to perform internal network port scanning and access cloud instance-metadata services.	5.0	More Details
CVE-2026-105137	A vulnerability was found in Laradock up to 20.4. Impacted is an unknown function of the file workspace/Dockerfile of the component Build Process. The manipulation results in download of code without integrity check. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2026-80464	Server-Side request forgery (SSRF) vulnerability in HAVELSAN Inc. Sef - AI Chatbot Platform allows Server Side Request Forgery. This issue affects Sef - AI Chatbot Platform: before 2.1. NOTE: The vendor was contacted and it was learned that the product is not supported.	4.9	More Details
CVE-2026-105676	Ghost is a Node.js content management system. From 1.20.0 until 6.64.0, a vulnerability in how Ghost loads theme translation files allowed an authenticated Administrator to read JSON files outside of the active theme's directory, potentially exposing server configuration secrets. This issue is fixed in version 6.64.0.	4.9	More Details
CVE-2026-105120	OpenAM before 16.1.3 contains an authorization bypass vulnerability in the sessions REST endpoint query operation that allows realm administrators to list sessions of every realm. Attackers holding delegated RealmAdmin privileges can supply a _queryFilter naming another realm to disclose usernames, universal IDs, and session handles across tenant boundaries.	4.9	More Details
CVE-2026-105121	OpenAM before 16.1.3 contains an improper authorization vulnerability that allows delegated administrators to destroy sessions outside their realms because realm checks use the requester's realm. Authenticated accounts holding the iplanet-am-session-destroy-sessions attribute can supply a target session identifier or handle to forcibly log out users in any realm.	4.9	More Details
CVE-2026-104417	Ghost from 1.20.0 before 6.64.0 contains a path traversal vulnerability in theme translation file loading that allows authenticated administrators to read JSON files outside the active theme directory. Attackers can manipulate the locale setting to load JSON files elsewhere on the server, exposing server configuration secrets.	4.9	More Details
CVE-2026-86817	The Five Star Business Profile and Schema WordPress plugin before 2.4.0 does not properly restrict the callbacks used to resolve schema field default values, allowing authenticated users with Author-level access and above to store input that discloses sensitive data, including other users' password hashes and arbitrary site option values, in public output readable by unauthenticated visitors.	4.9	More Details
CVE-2026-105645	Ghost is a Node.js content management system. From 5.37.0 until 6.67.0, a crafted request to the external media inliner could cause excessive CPU usage, making the Ghost server unresponsive. Exploiting this requires Administrator access. This issue is fixed in version 6.67.0.	4.9	More Details
CVE-2026-105646	Ghost is a Node.js content management system. From 4.0.0 until 6.67.0, a crafted content import file could cause excessive CPU usage, making the Ghost server unresponsive. Exploiting this requires Administrator access. This issue is fixed in version 6.67.0.	4.9	More Details

CVE-2026-102111	Kiteworks did not enforce the maximum permitted value for a configurable security-policy setting. An authenticated administrator could set this value outside its intended range so that the associated control never activated, while the control continued to appear enabled in the administrative interface and audit log, allowing it to be silently rendered ineffective.	4.9	More Details
CVE-2026-105687	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the delete-team-member RPC allows a team administrator to remove any member other than themselves but does not protect the team owner. A non-owner administrator can delete the owner's team-profile-rel membership and lock the owner out of the team and its projects, files, fonts, and media. This issue is fixed in version 2.18.0.	4.9	More Details
CVE-2026-102140	An authenticated administrator could initiate an administrative import using a file whose contents were not fully verified, because the import validated only the file's header rather than the complete file. This could allow unverified or forged content to be accepted and processed, affecting the integrity of the imported data.	4.9	More Details
CVE-2026-101357	The SEOPress – AI SEO Plugin & On-site SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'seopress_google_analytics_matomo_id' parameter in all versions up to, and including, 10.2 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. This requires an administrator to have delegated the Analytics management capability to the Subscriber role via the plugin's Advanced > Security settings.	4.9	More Details
CVE-2026-100272	In JetBrains YouTrack before 2026.2.19197 missing authorisation in the notification template preview allowed Project Administrators to read restricted issues	4.9	More Details
CVE-2026-78412	Velociraptor's WatchEvent gRPC API can specify the OrgId of the org from which events should be streamed. The server checks the API permissions against the caller's Org instead of the requested Org. This allows a user with API access in one org to read events from another org for which they have no access.	4.9	More Details
CVE-2026-97246	Subscriber PHP Object Injection in ShortPixel Image Optimizer <= 6.5.5 versions.	4.9	More Details
CVE-2026-100278	In JetBrains YouTrack before 2026.2.19197 users with restricted permission could edit and hide other users' comments	4.9	More Details
CVE-2026-92899	Apache WSS4J remembers the Nonce of each UsernameToken it accepts, so a captured token cannot be reused. It stored the Nonce as raw base64 text, but authentication decodes that text and uses the bytes. The same bytes can be written as base64 in several ways. An attacker who captured an authenticated request could re-send it with a space added to the Nonce: the password digest still verified, but the token no longer matched the remembered one, so the replay was accepted. Since a UsernameToken does not cover the message body, the captured token could then be reused on requests of the attacker's choosing until it expired. Affects deployments with a nonce replay cache configured, as Apache CXF has by default, and only tokens using a password digest. The cache is now keyed on the decoded Nonce. Users are recommended to upgrade to versions 4.0.2 or 3.0.6 or 2.4.4, which fix this issue.	4.8	More Details
CVE-2026-100265	In JetBrains Rider before 2026.2.1 al Assistant could auto-update third-party skills without user confirmation	4.8	More Details
CVE-2026-94484	Next.js is a React framework for building full-stack web applications. From 15.0.0 until 15.5.27 and 16.3.8, applications with a root-level catch-all page and statically generated or Incremental Static Regeneration routes can use a shared response cache key that is insufficiently scoped to the source route. A single unauthenticated crafted request can poison that cache, causing cross-user content substitution or persistent denial of service until the poisoned entry is revalidated or replaced. This issue is fixed in versions 15.5.27 and 16.3.8.	4.8	More Details
CVE-2026-104419	Zebra (zebrad) 4.5.0 before 6.3.0 discards which peer supplied the block hashes in FindBlocks responses, then assigns 100 misbehavior points, the ban threshold, to whichever peer serves a requested block more than 50,000 heights above the tip. A remote peer can return real far-ahead hashes to a syncing node so that honest peers get banned, eroding its peer set and raising eclipse risk.	4.8	More Details
CVE-	YesWiki before 4.6.7 contains an insufficient session expiration vulnerability that allows attackers to		

2026-104468	reuse old password reset links because tokens lack expiry timestamps. Attackers who obtain an unused reset URL from mailboxes, logs, backups, or browser history can submit a new password through checkEmailKey() and take over accounts.	4.8	More Details
CVE-2026-9864	Fortra BoKS Server Agent contains a predictable password generation vulnerability in the adjoin utility. Machine-account passwords generated during Active Directory join or password renewal operations may have significantly less entropy than intended, making them more susceptible to prediction by an attacker who can estimate when the password was generated.	4.8	More Details
CVE-2026-105249	A weakness has been identified in vgmstream up to r2117. This impacts the function make_group_random of the file src/meta/txtprocess.c of the component TXTP File Handler. This manipulation causes use after free. The attack needs to be launched locally. Patch name: ae37662ad626254ddd96ad69ac263792d7a92024. It is recommended to apply a patch to fix this issue.	4.8	More Details
CVE-2026-103113	A vulnerability was determined in OS4ED openSIS-Classic up to 9.3. The affected element is the function save action of the file modules/students/Student.php of the component General Information Tab. Executing a manipulation of the argument students can lead to sql injection. 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.	4.7	More Details
CVE-2026-100184	The Calculated Fields Form – AI Form Builder for WordPress – Contact, Payment, Quote, Quiz & More plugin for WordPress is vulnerable to Reflected DOM-Based Cross-Site Scripting via the 'x (attacker-chosen name matching the form's url.<name> predefined value)' parameter in all versions up to, and including, 5.5.1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires that the targeted form has a Text Area field configured with a 'url.<name>' Predefined Value and predefinedClick disabled, which is a documented and commonly used plugin feature.	4.7	More Details
CVE-2026-102846	A vulnerability was detected in gedelung HospitalManagement up to c2d45543789a3887067d3915f69d44cfc2cf76a8. Impacted is the function sistem.php::simpan of the file application/modules/admin/controllers/sistem.php of the component Configuration Handler. The manipulation of the argument tipe/title/content_setting results in improper authorization. The attack may be launched remotely. The exploit is now public and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-105146	A vulnerability was found in Comsenz Discuz! X5.0-20260801/X5.0-20260820/X5.0-20260910. Affected by this issue is the function modmedalsubmit of the file upload/source/app/admin/child/medals/mod.php of the component Admin Medal Moderation. The manipulation of the argument delete results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-105118	OpenAM before 16.1.3 contains an open redirect vulnerability that allows unauthenticated attackers to redirect users by supplying an unverified id_token_hint to the /oauth2/connect/endTime endpoint. Attackers can name any realm client in a forged hint to redirect victims to any registered post-logout URI, enabling phishing that borrows the OpenAM host's trust.	4.7	More Details
CVE-2026-105263	A security flaw has been discovered in Shaarli up to 0.16.3. The affected element is the function MetadataController of the file application/front/controller/admin/MetadataController.php of the component Admin Metadata Endpoint. Performing a manipulation of the argument url results in server-side request forgery. The attack may be initiated remotely. Upgrading to version 0.16.4 is sufficient to fix this issue. The patch is named 8ca4de8e7c932a684481f5fbb1229fe16de1f4d2. It is advisable to upgrade the affected component.	4.7	More Details
CVE-2026-105315	A vulnerability has been found in django-haystack up to 3.3.0. Affected is the function _to_python of the file haystack/backends/elasticsearch_backend.py of the component more_like_this Template Tag Handler. Such manipulation of the argument result_class leads to improper neutralization of directives in dynamically evaluated code. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.4.0 is able to address this issue. The name of the patch is eb05f193c9771a68dcc8cfac6674a0d48a52ee9d. It is suggested to upgrade the affected component.	4.7	More Details
CVE-2026-103117	A security vulnerability has been detected in OS4ED openSIS-Classic up to 9.3. Affected is the function db_properties of the file functions/Databaselnc.php of the component Save Data Handler. Such manipulation of the argument values leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early	4.7	More Details

	through an issue report but has not responded yet.		
CVE-2026-87970	The If-So Dynamic Content WordPress plugin before 1.10.2 does not escape a request-supplied value before reflecting it in an unauthenticated AJAX response that is served as HTML, allowing attackers to execute arbitrary JavaScript in the browser of a visitor who opens a crafted link.	4.7	More Details
CVE-2026-105176	A vulnerability was determined in SourceCodester Drug Recommendation System 1.0. Impacted is an unknown function of the file /Admin/edit_class.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-100263	In JetBrains YouTrack before 2026.2.18991 stored HTML injection via the User-Agent header was possible	4.7	More Details
CVE-2026-105226	A security flaw has been discovered in osCommerce osCommerce2 up to 2.3.4.1. This vulnerability affects the function include of the file admin/newsletters.php of the component Newsletter Management. Performing a manipulation of the argument module results in code injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-102912	A vulnerability was identified in SourceCodester Online Leave Management System 1.0. This issue affects some unknown processing of the file /admin/?page=reports. The manipulation of the argument date_start/date_end leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-102843	A security flaw has been discovered in gedelung HospitalManagement up to c2d45543789a3887067d3915f69d44cfc2cf76a8. This affects the function hapus of the file application/modules/admin/controllers/data_galeri.php of the component Endpoint. Performing a manipulation of the argument gbr results in path traversal. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-105177	A vulnerability was identified in SourceCodester Drug Recommendation System 1.0. The affected element is an unknown function of the file /Admin/add_drug.php of the component Drug Creation. Such manipulation of the argument txtname/cmdtype/txtusage/txtsideeffect/cmdcontraindication leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-105178	A security flaw has been discovered in SourceCodester Drug Recommendation System 1.0. The impacted element is the function mysqli_real_escape_string of the file /Admin/add_symptom.php of the component Symptom Creation. Performing a manipulation of the argument txtname results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-39600	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Mehul Gohil Aculect AI Companion aculect-ai-companion allows Phishing.This issue affects Aculect AI Companion: from n/a through 0.8.1.	4.7	More Details
CVE-2026-102107	Kiteworks Core contains a business logic flaw in a Kiteworks file-request feature allowed an authenticated user to send a request that appeared to originate from another user, because the server did not verify that the requester was authorized to act as the specified account. This could be used to solicit files or information from a recipient under a trusted identity; exploitation requires the feature to be enabled for the attacker's profile and the targeted recipient to act on the request.	4.6	More Details
CVE-2026-102581	A flaw was found in Moodle. Insufficient output escaping in templates used to display forum posts enables a stored cross-site scripting (XSS) vulnerability. An attacker can inject malicious content into a forum post, which then executes arbitrary script code in the browser of another user viewing the affected post.	4.6	More Details
CVE-2026-47526	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the firmware where an attacker could cause a null pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	4.4	More Details
	The SMBus driver API exposed smbusr_remove_cb() and smbusr_notify_remove_cb() as Zephyr syscalls. Their verifiers in drivers/smbusr/smbusr_handlers.c validated only the dev argument with K_SYSCALL_OBJ(dev, K_OBJ_DRIVER_SMBUS) and forwarded the caller-supplied struct		

CVE-2026-17053	smbus_callback *cb pointer into kernel-mode driver code without any K_SYSCALL_MEMORY_READ/K_SYSCALL_MEMORY_WRITE validation. A companion change in 2023 had already removed the matching smbus_smbalert_set_cb() / smbus_host_notify_set_cb() syscalls for this reason, but the two removal syscalls were left exposed. On a build with CONFIG_USERSPACE=y, CONFIG_SMBUS=y and a driver implementing the callback operations (drivers/smbus/intel_pch_smbus.c with CONFIG_SMBUS_INTEL_PCH_SMBALERT/CONFIG_SMBUS_INTEL_PCH_HOST_NOTIFY, or drivers/smbus/smbus_stm32.c with CONFIG_SMBUS_STM32_SMBALERT), any user-mode thread that has been granted the SMBus device object can invoke these syscalls with an arbitrary pointer. The value reaches smbus_callback_remove() in drivers/smbus/smbus_utils.h, which uses it as a node identity against the kernel's sys_slist_t of registered callbacks. The consequence is that an unprivileged thread can unregister an SMBALERT or Host Notify callback that a supervisor-mode component registered, silently disabling alert handling for the rest of the system; because Zephyr images have fixed symbol addresses and the syscall returns 0 on a hit versus -ENOENT on a miss, the target address is both derivable and searchable. In builds with CONFIG_ASSERT=y the __ASSERT(callback->handler, ...) check additionally dereferences the caller-supplied address in supervisor mode, so a bogus pointer raises a kernel-mode fault and a fatal system error, and the fault/no-fault outcome discloses which addresses are mapped. The fix removes both syscall entry points, demoting the two functions to ordinary static inline calls so that callback list manipulation is available only to supervisor-mode code. There is no impact on builds without CONFIG_USERSPACE, and no impact on configurations that do not enable an SMBus driver with SMBALERT or Host Notify support.	4.4	More Details
CVE-2026-47562	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where a user could inject crafted text into the kernel log because the supplied version string is not properly sanitized. A successful exploit of this vulnerability might lead to denial of service and data tampering.	4.4	More Details
CVE-2026-93832	A component of one of the Motorola system applications was exported without permission, allowing for the revocation of runtime permissions from other apps.	4.4	More Details
CVE-2026-101893	Newell Brands DYMO ID 1.5.1.71 parses job files using XmlDocument.Load() without disabling DTD processing. The PC Job Files view automatically parses every recognized job file extension on folder browse. A crafted file on any browsed network share can perform SSRF, capture NTLMv2 credentials, read local files, or crash the process. Fixed in 1.6.0.	4.4	More Details
CVE-2026-91072	The EWWW Image Optimizer WordPress plugin before 8.8.0 does not confine a WebP-derivative file migration routine to the current site's own uploads directory, letting an attacker with Administrator-level access rename or delete existing WebP-derivative image files outside that scope, including, on a multisite network, files belonging to a different site they have no access to.	4.4	More Details
CVE-2026-47531	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer where an attacker could cause a null pointer dereference. A successful exploit of this vulnerability might lead to denial of service.	4.4	More Details
CVE-2026-105291	A vulnerability was identified in feelec-yishu feelcrm-os 1.0.0. This vulnerability affects the function GroupController::index of the file App/Feelcrm/Index/Controller/GroupController.class.php of the component Department Search Endpoint. The manipulation of the argument keyword leads to cross site scripting. The attack can be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-105678	Ghost is a Node.js content management system. From 0.5.0 until 6.64.0, staff users with the Editor or Super Editor role were able to assign their own role to Author and Contributor users, despite not having permission to assign that role. This issue is fixed in version 6.64.0.	4.3	More Details
CVE-2026-105288	A vulnerability has been found in feelec-yishu feelcrm-os 1.0.0. Affected by this vulnerability is the function IndexController::index of the file App/ThinkPHP/Common/functions.php of the component Crm Endpoint. Such manipulation of the argument redirect_url leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-102122	Kiteworks did not correctly enforce which roles a shared folder's manager was permitted to assign. In a default configuration, an authenticated user holding the Manager role on a folder could grant the Owner role to themselves or to other members of that folder.	4.3	More Details
CVE-2026-79618	The WP User Frontend WordPress plugin before 4.3.12 does not enforce its subscription-purchase requirement in one of its post-creation handlers, allowing authenticated users with subscriber-level access and above to create and, depending on the form's configuration, immediately publish posts through forms restricted to paying subscribers.	4.3	More Details
CVE-	In JetBrains YouTrack before 2026.2.18991 sSRF via stored XHTML injection was possible during PDF		More

2026-100257	export	4.3	Details
CVE-2026-103629	Integer overflow in Skia in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-104982	A flaw has been found in Linux Mint Xreader up to 4.6.5. This issue affects the function <code>setup_document_content_list/g_strdup_printf</code> of the file <code>backend/epub/epub-document.c</code> of the component EPUB File Handler. This manipulation causes path traversal. The attack is possible to be carried out remotely. The exploit has been published and may be used. Upgrading to version 4.6.6 is capable of addressing this issue. Patch name: <code>a5aecea074e8564b7a22f1ce054b31ec862974b7</code> . It is advisable to upgrade the affected component. One of the project maintainers explains, that "EPUB support was removed from Xreader and reimplemented in Xepub".	4.3	More Details
CVE-2026-39763	Missing Authorization vulnerability in Deepak Anand WP Dummy Content Generator <code>wp-dummy-content-generator</code> allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Dummy Content Generator: from n/a through 4.0.0.	4.3	More Details
CVE-2026-102847	A flaw has been found in gedelumbung HospitalManagement up to <code>c2d45543789a3887067d3915f69d44cfc2cf76a8</code> . The affected element is the function <code>kirim</code> of the file <code>application/modules/web/controllers/buku_tamu.php</code> of the component Guest Book. This manipulation of the argument <code>nama/email/pesan</code> causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-97343	The Burst Statistics – Simple WordPress Analytics (Google Analytics Alternative) plugin for WordPress is vulnerable to Improper Authentication leading to Account Persistence in all versions up to, and including, 3.7.1. This is due to the <code>`maybe_load_shared_dashboard()`</code> handler issuing a genuine WordPress session cookie for the <code>`burst_statistics_viewer`</code> account to any visitor presenting a valid share token via <code>`wp_set_auth_cookie()`</code> , while the plugin only blocks Application Passwords for the resulting <code>`burst_viewer`</code> role and does not restrict the core <code>`/wp-json/wp/v2/users/me`</code> password update endpoint or filter the <code>`edit_user`</code> capability for that account — leaving WordPress core's built-in rule that any authenticated user may update their own account fully in effect. This makes it possible for unauthenticated attackers to set an attacker-chosen password on the <code>`burst_statistics_viewer`</code> WordPress account, constituting a permanent takeover of that limited-privilege (<code>`view_burst_statistics`</code>) account that persists through share-token revocation, share-token expiration, and execution of the plugin's daily <code>`cleanup_viewer_sessions()`</code> routine. Exploitation requires that the attacker have obtained a valid <code>`burst_share_token`</code> , such as one that has been shared publicly or distributed to an untrusted party.	4.3	More Details
CVE-2026-103495	In JetBrains YouTrack before 2026.2.19422 missing authorisation allowed reloading of translation catalogs	4.3	More Details
CVE-2026-13719	An authenticated user can list alert rules stored in folders they are not allowed to read through the alert rules API list endpoint. When the set of folders the user may read was empty, the folder restriction was dropped and every alert rule in the organization was returned. From Grafana 13.1.0, any user can trigger this with a folder filter. The exposed data is rule configuration; data source credentials are not exposed.	4.3	More Details
CVE-2026-102090	Kiteworks Core before version 9.5.1 is vulnerable to Content Injection. A URL parameter in the PDF viewer was insufficiently validated, allowing an attacker-controlled document to be loaded and displayed under the trust of the legitimate application domain. This could increase the credibility of phishing attempts relying on malicious links embedded in the displayed content.	4.3	More Details
CVE-2026-94180	Authorization Bypass Through User-Controlled Key vulnerability in Monetizemore Advanced Ads allows Retrieve Embedded Sensitive Data. This issue affects Advanced Ads: from n/a through 2.0.26.	4.3	More Details
CVE-2026-105250	A security vulnerability has been detected in vgmstream up to r2117. Affected is the function <code>decode_ms_ima</code> of the file <code>src/coding/ima_decoder.c</code> of the component Microsoft IMA Decoder. Such manipulation leads to divide by zero. The attack can be executed remotely.	4.3	More Details
CVE-2026-103396	bbs-go through 4.4.6 contains a permission bypass vulnerability in the AdminMiddleware authorization logic where the <code>read-only dashboard.user.view</code> permission rule matches the <code>/api/admin/user/synccount</code> endpoint before the intended <code>dashboard.user.update</code> rule. Authenticated users with only view permissions can call the <code>synccount</code> endpoint to trigger expensive full-table user recounts and cache	4.3	More Details

	invalidations, causing denial of service through repeated concurrent database operations.		
CVE-2026-100269	In JetBrains YouTrack before 2026.2.19197 helpdesk project's Authorized Reporters list could be bypassed	4.3	More Details
CVE-2026-39783	Missing Authorization vulnerability in WP SYNTAX Polylang polylang allows Retrieve Embedded Sensitive Data.This issue affects Polylang: from n/a through 3.8.7.	4.3	More Details
CVE-2026-104612	A vulnerability was found in SourceCodester Student Result Management System 1.0. This affects an unknown part of the file script/academic/core/new_announcement.php of the component Announcement Module. The manipulation of the argument title/announcement results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2026-91108	The Alt Text AI - Automatically generate image alt text for SEO and accessibility plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.10.41. 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 overwrite the post_content of any post or page on the site — including content they do not own — with LLM-generated text influenced by attacker-controlled keywords, enabling black-hat SEO manipulation and unauthorized consumption of the site owner's paid AltText.ai API credits. The nonce required to invoke the action is emitted on every admin page including /wp-admin/profile.php, which is accessible to Subscribers, making the nonce trivially obtainable by any authenticated user.	4.3	More Details
CVE-2026-104675	Missing Authorization vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through 5.30.0.	4.3	More Details
CVE-2026-105157	A security vulnerability has been detected in RainyGao DocSys up to 2.02.85. The affected element is the function DocController.doGetTmp of the file /Doc/doGetTmpFile.do of the component Document Controller. The manipulation of the argument path/fileName leads to path traversal. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-100258	In JetBrains YouTrack before 2026.2.18991 missing authorisation allowed read-only users to read project settings	4.3	More Details
CVE-2026-51878	deeptutor 1.4.0 contains an authorization bypass through a user-controlled object identifier in TurnRuntimeManager.regenerate_last_turn. A remote caller can enumerate or obtain a session_id and trigger regenerate on another user's session.	4.3	More Details
CVE-2026-102579	A flaw was found in Moodle. An incorrect capability check in the grade web service allows an authenticated student to access profile information of other students enrolled in the same course that they should not have permission to view. This issue leads to unauthorized information disclosure.	4.3	More Details
CVE-2026-103078	Authorization Bypass Through User-Controlled Key vulnerability in Ahmad JS Help Desk js-support-ticket allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JS Help Desk: from n/a through 4.0.0.	4.3	More Details
CVE-2026-103057	AiSOC versions 5.1.0 before 12.0.0 contain an authentication bypass vulnerability in the realtime service internal endpoints POST /internal/agent-event and POST /internal/push. Attackers can post arbitrary events with spoofed tenant identifiers to broadcast malicious content over WebSocket and Redis SSE channels or send unauthorized notifications to registered devices.	4.3	More Details
CVE-2026-105062	Missing Authorization vulnerability in Brandtoss WP Admin Audit wp-admin-audit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Admin Audit: from n/a through 1.2.17.	4.3	More Details
CVE-2026-97219	The MStore API WordPress plugin before 4.22.1 does not restrict which fields of an order a customer may update, allowing any authenticated user with a self-registerable account to change the status of their own unpaid order to a paid or fulfilled state and receive the goods without paying.	4.3	More Details
CVE-2026-105225	A vulnerability was identified in osCommerce osCommerce2 up to 2.3.4.1. This affects the function include of the file includes/classes/payment.php of the component Payment Page. Such manipulation of the argument MODULE_PAYMENT_INSTALLED leads to code injection. The attack can be executed remotely. The exploit is publicly available and might be used. The project was informed of the problem	4.3	More Details

	early through an issue report but has not responded yet.		
CVE-2026-103265	Fleet versions before 4.89.0 fail to properly filter MDM command results by team authorization in the commands/results endpoint. Team-scoped users can read MDM command results for hosts on other teams when a shared command UUID targets hosts across multiple teams, exposing host UUIDs, command payloads, and device responses.	4.3	More Details
CVE-2026-102577	A flaw was found in Moodle. Incorrect handling of IPv4-mapped IPv6 addresses within the URL downloader's host-blocking logic allows an authenticated remote user to bypass blocked-host restrictions. By supplying a crafted URL, an attacker can induce the server to make requests to restricted destinations, leading to Server-Side Request Forgery (SSRF).	4.3	More Details
CVE-2026-102584	A flaw was found in Moodle. Due to a missing capability check, a low-privileged authenticated user can trigger the recalculation of grade penalties without holding the required permissions. This issue allows unauthorized users to modify grade penalty records, potentially altering student assessment scores.	4.3	More Details
CVE-2026-102585	A flaw was found in Moodle. When enrolling a user into a course while assigning them to a group, the application does not verify whether the selected group actually belongs to that course. An authenticated user with teacher privileges could exploit this flaw to add users to groups within courses they do not have authorization to access.	4.3	More Details
CVE-2026-105098	A security flaw has been discovered in Omega Solution CoinEx Crypto 2025. Affected is an unknown function of the file /ticket/customer of the component Support Ticket API. The manipulation of the argument status/page/count results in information disclosure. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The product web site does not exist anymore. Maybe the product got retired and/or replaced. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-103387	A weakness has been identified in garycourt uri-js up to 4.4.1. This affects the function URI.parse of the file src/schemes/mailto.ts of the component Mailto Header Handler. This manipulation of the argument to causes uncaught exception. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-104402	Insertion of Sensitive Information Into Sent Data vulnerability in farvisun Mindio Magic MCP mindio-magic-mcp allows Retrieve Embedded Sensitive Data.This issue affects Mindio Magic MCP: from n/a through 0.5.6.	4.3	More Details
CVE-2026-105097	A vulnerability was identified in Omega Solution CoinEx Crypto 2025. This impacts an unknown function of the file /customer-currency/ of the component Customer Information API. The manipulation of the argument ID leads to authorization bypass. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The product web site does not exist anymore. Maybe the product got retired and/or replaced. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-105684	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the get-comment-threads, get-comment-thread, and get-comments RPC commands use check-comment-permissions! but do not apply the share link's pages restriction. A holder of a page-scoped share link can retrieve comment threads and full comment bodies from other pages in the same file, including commenter names, email addresses, photos, and page identifiers. The disclosed page identifiers can also be used with affected page-reading functionality to access unshared design content. This issue is fixed in version 2.18.0.	4.3	More Details
CVE-2026-102586	A flaw was found in Moodle. Insufficient sanitization of username input on the password reset page allows a remote attacker to conduct a cross-site scripting (XSS) attack. By convincing an unauthenticated user to access a specially crafted password reset link, an attacker could execute arbitrary script in the victim's browser.	4.3	More Details
CVE-2026-103542	A flaw has been found in formtools.org Form Tools up to 3.1.1. Impacted is the function smart_fill of the file /global/code/actions.php of the component AJAX Endpoint. This manipulation of the argument url causes server-side request forgery. The attack can be initiated remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-104451	YesWiki before 4.6.7 contains a cross-site request forgery vulnerability in RevisionsHandler that allows attackers to restore old page revisions through GET requests lacking CSRF token validation. Attackers can lure write-capable users into a top-level navigation with the restoreRevisionId parameter, silently overwriting current page content with stale or vandalized revisions.	4.3	More Details
	The Redux Framework plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.5.14 This is due to the plugin not properly verifying that a user is authorized to perform		

CVE-2026-88999	an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary media library attachments, including administrator-owned files, from the affected site. This is exploitable by Subscribers when a Custom Fonts field is registered on the user profile page via Redux_Users::set_profile(), as doing so causes the required redux_custom_fonts nonce to be rendered into the Subscriber's wp-admin/profile.php page.	4.3	More Details
CVE-2026-100259	In JetBrains YouTrack before 2026.2.18991 improper access control on Gantt chart allowed edits by users with view-only access	4.3	More Details
CVE-2026-104401	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Memberful Memberful - Membership Plugin memberful-wp allows Retrieve Embedded Sensitive Data.This issue affects Memberful - Membership Plugin: from n/a through 1.81.2.	4.3	More Details
CVE-2026-105438	A flaw has been found in O2OA up to 10.0.1-ce. This affects the function ActionUploadExcelWithURL of the file /x_general_assemble_control/jaxrs/excel/upload/with/url of the component General Module. Executing a manipulation of the argument fileUrl can lead to server-side request forgery. 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.	4.3	More Details
CVE-2026-1661	The WP Mail Logging WordPress plugin before 1.17.0 does not properly restrict the HTML and CSS of logged emails before rendering them in its admin log screens, allowing unauthenticated users to inject styled content and links, for example through a public contact form, that can deceive an administrator viewing the log and send their browser to an attacker-controlled page.	4.3	More Details
CVE-2026-56098	A flaw was found in rubygem-katello. The RegistryProxiesController in Katello contains an authorization bypass vulnerability due to an execution fall-through in the registry_authorize filter. While the application identifies unauthorized requests and triggers an error response via the unauthorized method, it fails to halt the execution of the current code path (missing return statement). This failure in the control flow allows the application to proceed into subsequent business logic and database validation filters. Consequently, the application reveals its internal state through differential responses, allowing an unprivileged attacker to enumerate valid Users, Organizations, and Products across the entire instance.	4.3	More Details
CVE-2026-105029	UVdesk support-center-bundle before 1.1.3.3 contains an insecure direct object reference vulnerability in the rateTicket action of Controller/Ticket.php that allows authenticated customers to rate other customers' tickets. Attackers can supply arbitrary ticket IDs, which are loaded without an ownership check, to submit or change satisfaction ratings on tickets owned by other customers.	4.3	More Details
CVE-2026-97267	Subscriber Broken Access Control in Prevent files / folders access <= 2.6.7 versions.	4.3	More Details
CVE-2026-103284	Ghost versions from 5.125.1 before 6.57.1 contain an information disclosure vulnerability in the Admin Feedback endpoint that allows unauthorized staff users to access member data. Attackers with staff privileges can query the feedback endpoint to retrieve sensitive member information without proper authorization checks.	4.3	More Details
CVE-2026-103282	Ghost versions 0.5.0 before 6.23.0 contain a concurrency issue in the staff invitation acceptance mechanism that allows multiple accounts to be created from a single invite token. Attackers can exploit this race condition by submitting concurrent requests with the same invitation token to create duplicate user accounts.	4.3	More Details
CVE-2026-104963	Plane is an open-source project management tool. Prior to 1.4.0, GET /api/workspaces/{slug}/cycles/ through WorkspaceCyclesEndpoint and GET /api/workspaces/{slug}/modules/ through WorkspaceModulesEndpoint return records from every project in a workspace without checking whether the requester belongs to each project. Any authenticated workspace member, including a Guest with access to only one project, can enumerate names, descriptions, sprint dates, issue counts, progress snapshots, external integration IDs, linked URLs, and member lists for cycles and modules in private projects. The sibling WorkspaceLabelsEndpoint and WorkspaceStatesEndpoint apply the correct project__project_projectmember__member=request.user filter, making the cycle and module endpoints inconsistent outliers. This issue is fixed in 1.4.0.	4.3	More Details
CVE-2026-66247	iControl is affected by an insecure Cross-Origin Resource Sharing (CORS) policy vulnerability, which could allow a malicious website to execute cross-origin requests with included credentials, enabling an attacker to access and exfiltrate sensitive data within the context of the victim's active session.	4.3	More Details
CVE-2026-	Missing Authorization vulnerability in ThimPress LearnPress learnpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LearnPress: from n/a through 4.4.9.1.	4.3	More Details

39717			
CVE-2026-85576	The All in One Files Upload WordPress plugin before 2.0.17 does not have any capability check, and does not verify the authenticity of the request, when saving its settings, allowing any authenticated user, such as a subscriber, to change them.	4.3	More Details
CVE-2026-105046	Kentico Xperience 13 before 13.0.216 lacks object-level authorization checks for administration API endpoints.	4.3	More Details
CVE-2026-103621	Integer overflow in Compositing in Google Chrome prior to 154.0.8037.97 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2025-31980	HCL BigFix Service Management is affected by an Improper Input Validation vulnerability, which could allow an attacker to inject unvalidated, malformed data into the application, enabling potential injection attacks or errors in downstream processing systems.	4.3	More Details
CVE-2026-103275	Ghost 5.42.2 before 6.58.0 contains an information disclosure vulnerability in the Admin API bulk post and page edit and delete endpoints, which accept filters on restricted fields such as authors.password, because of an incomplete fix for CVE-2026-70590. Staff-level attackers can infer other staff users' password hashes from which filters match and perform offline password-guessing attacks against them.	4.3	More Details
CVE-2026-103285	Ghost versions from 5.19.0 before 6.57.1 contain a cross-site request forgery vulnerability in the post feedback functionality that allows attackers to submit feedback on behalf of logged-in users. Attackers can craft a malicious link to the feedback page that automatically submits feedback when visited by authenticated members without their knowledge or consent.	4.3	More Details
CVE-2026-103273	Ghost versions 4.3.0 before 6.58.0 contain an authentication bypass vulnerability where lower-privilege staff users can use staff tokens to bypass post editing restrictions. Attackers with staff credentials can leverage tokens to edit posts beyond their assigned privilege level.	4.3	More Details
CVE-2026-11399	The Helpdesk Support Ticket System for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.1.6 via the 'id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary ticket responses belonging to other users by supplying any stsw_responses row ID to the deletion handler after obtaining the nonce from the admin footer.	4.3	More Details
CVE-2026-102670	Joyland AI app explicitly permits cleartext HTTP traffic on Android 9+ where the default is to block it.	4.3	More Details
CVE-2026-104894	Plane is an open-source project management tool. Prior to 1.4.0, the modules endpoint accepts issue UUIDs in the URL path without validating that they belong to the caller's workspace. An authenticated user can link issues from any workspace to modules in their own workspace. This issue is fixed in 1.4.0.	4.3	More Details
CVE-2026-51899	In SuperAGI v0.0.14 and prior, controller endpoints (/api/agents/create, /api/agents/schedule, /api/agents/delete, /api/agents/edit_schedule, /api/agents/stop_schedule) allow authenticated users from one organization to create, schedule, edit, stop, and delete agents belonging to a different organization's project. The endpoints accept a project_id parameter but do not verify that the project belongs to the authenticated user's organization.	4.3	More Details
CVE-2026-85004	The Popup Maker WordPress plugin through 1.4.5 does not perform a capability check on one of its account-connection actions, only verifying a nonce, allowing authenticated users with minimal privileges such as Subscribers to overwrite a site-wide Popup Maker WordPress plugin through 1.4.5 option (the linked service account and API configuration) that should only be modifiable by administrators.	4.3	More Details
CVE-2026-89190	The Robin Image Optimizer WordPress plugin before 2.0.8 does not check the user's capabilities before dispatching one of its bundled admin framework's request handlers, allowing users with a subscriber-level account to render admin-only Robin Image Optimizer WordPress plugin before 2.0.8 pages and disclose the Robin Image Optimizer WordPress plugin before 2.0.8's stored settings.	4.3	More Details
CVE-2026-103118	A vulnerability was detected in GraphicsMagick up to 1.3.47. Affected by this vulnerability is the function ExtractPostscript of the file coders/wpg.c of the component WPG File Handler. Performing a manipulation results in uncontrolled recursion. The attack may be initiated remotely. The patch is named 627b5b1b2fc2. It is suggested to install a patch to address 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-2026-104412	Ghost 0.5.0 before 6.64.0 does not correctly restrict staff role assignment, allowing users with the Editor or Super Editor role to assign their own role to other staff despite lacking permission to do so. An authenticated Editor or Super Editor can promote Author and Contributor users to Editor or Super Editor.	4.3	More Details
CVE-2026-97074	Subscriber Insecure Direct Object References (IDOR) in Newsletters, Email Marketing, SMS and Popups by Omnisend <= 1.9.0 versions.	4.3	More Details
CVE-2026-42528	A memory calculation bug in mod_dav in Apache httpd 2.4.67 and earlier allows an attacker with permission to create WebDAV locks to crash server child processes. Users are recommended to upgrade to version 2.4.69, which fixes this issue	4.3	More Details
CVE-2026-97079	Subscriber Insecure Direct Object References (IDOR) in Webba Booking <= 6.5.0 versions.	4.3	More Details
CVE-2026-90953	The Image Optimizer WordPress plugin before 1.7.7 does not enforce its intended capability check on several of its read REST routes, allowing any authenticated user to read attachment metadata and site-wide statistics that should be restricted to administrators.	4.3	More Details
CVE-2026-102382	Authorization Bypass Through User-Controlled Key vulnerability in Ahmad Majestic Support majestic-support allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Majestic Support: from n/a through 1.2.0.	4.3	More Details
CVE-2026-103267	Ghost versions before 6.62.0 contain an authentication bypass vulnerability in staff invite acceptance that allows users to specify any email address when creating their account. Attackers can accept leaked invite tokens with attacker-controlled email addresses, or legitimate recipients can register with unintended email providers.	4.3	More Details
CVE-2026-94672	Contributor Insecure Direct Object References (IDOR) in Safe SVG <= 2.5.0 versions.	4.3	More Details
CVE-2026-94544	Next.js is a React framework for building full-stack web applications. From 16.3.0 until 16.3.8, pending use cache fills for the same key are shared without separating Draft Mode requests from regular requests. An overlapping regular request can receive unauthenticated unpublished content from an editor's Draft Mode fill, while an overlapping Draft Mode request can receive published content from a regular fill. When the regular request prerenders a page, the draft-dependent content can persist in the generated page and be served to later visitors until revalidation. Sites are affected when Cache Components or experimental.useCache is enabled and cached functions return draft-dependent content. This issue is fixed in version 16.3.8.	4.2	More Details
CVE-2026-102576	A flaw was found in Quay. A remote attacker could trick a user into logging in through a crafted link, resulting in cross-site scripting (XSS). Because the application does not validate the redirect destination before navigating, this flaw allows the execution of arbitrary script in the context of the victim's authenticated browser session. Successful exploitation requires the target Quay deployment to use direct database authentication and the victim to complete login through the malicious URL.	4.2	More Details
CVE-2026-96825	Subscriber Bypass Vulnerability in All In One WP Security & Firewall <= 5.4.8 versions.	4.2	More Details
CVE-2026-103533	A vulnerability was found in David-Crty databasement up to 1.7.1. This impacts the function https://github.com/David-Crty/databasement/pull/511 of the file <code>app/Http/Requests/Api/V1/RestoreRequest.php</code> of the component database-servers API Endpoint. The manipulation of the argument <code>schema_name</code> results in path traversal. The attack may be launched remotely. A high complexity level is associated with this attack. The exploitability is said to be difficult. The exploit has been made public and could be used. Upgrading to version 1.7.2 will fix this issue. You should upgrade the affected component.	4.1	More Details
CVE-2026-102137	An authenticated administrator could bypass the content validation applied to an administrative file upload and store a file containing dangerous content on the appliance. This did not by itself result in code execution, which would require a separate vulnerability to run the stored file.	4.1	More Details
CVE-2026-105301	A flaw was found in the X.509 client-certificate authenticator of Keycloak, a solution for identity and access management. The issue occurs when the server is configured to check certificate revocation using CRL Distribution Points or OCSP. An attacker can provide a specially crafted certificate that points to a malicious server, causing Keycloak to make unauthorized outbound requests to internal or external endpoints before the certificate is fully validated. This can lead to a blind server-side request forgery	4.0	More Details

	(SSRF) attack.		
CVE-2026-103260	n8n versions before 2.39.6 and 2.40.0 before 2.40.1 contain an approval bypass vulnerability in the Send and Wait node's Approve Within Chat mode. Attackers can submit resume requests without verification of the requester's identity or approval permissions, allowing unauthenticated users to advance waiting executions and trigger guarded actions.	4.0	More Details
CVE-2026-77387	geopy is a geocoding library for Python. Prior to 2.5.0, geopy.Point and Point.from_string() can spend excessive CPU time due to inefficient regular-expression behavior when an application passes a long malformed coordinate string without the 256-character input limit used by the fix. Geocoder reverse methods also reach the vulnerable parsing path when called with string inputs. Repeated attacker-controlled requests can cause a denial of service, while the numeric Point constructor is unaffected. This issue is fixed in version 2.5.0.	4.0	More Details
CVE-2026-105647	Ghost is a Node.js content management system. From 6.54.1 until 6.65.0, a validation issue allowed some functionality, such as Webmentions, to be abused by an unauthenticated user to make limited HTTP requests to hosts in the Ghost server's internal network. A successful attack would not result in any response data being returned. This issue is fixed in version 6.65.0.	4.0	More Details
CVE-2026-105048	The Playground feature of Zilliz Attu before 3.0.0 allows SSRF (proxying of requests to private IP addresses).	4.0	More Details
CVE-2026-94594	Armatura One's message broker logs client connection credentials and the associated password in plain text during normal operation. Any party with read access to this log, or to a backup or support bundle that includes it, can obtain the logged credential.	4.0	More Details
CVE-2026-105648	Ghost is a Node.js content management system. From 6.0.9 until 6.65.0, a validation issue allowed some functionality, such as Webmentions, to be abused by an unauthenticated user to make limited HTTP requests to hosts in the Ghost server's internal network on some network configurations. A successful attack would not result in any response data being returned. This issue is fixed in version 6.65.0.	4.0	More Details
CVE-2026-105083	ImageMagick before 7.1.2-32 and 6.9.13-57 contains a policy bypass vulnerability in LoadPolicyCache that silently skips security policy rules when policy.xml uses an alternate DOCTYPE. A valid DOCTYPE not ending in 'J]>' makes the parser consume the rest of the file, so no policy rules are applied and restricted operations become allowed.	3.9	More Details
CVE-2026-103290	Ghost versions 6.14.0 through versions prior to 6.27.0 contain a path traversal vulnerability in the ImageSize service. Insufficient input validation of user-supplied file paths may allow authenticated staff users to access local files outside the intended data storage directories on the server.	3.8	More Details
CVE-2026-105683	Ghost is a Node.js content management system. From 6.14.0 until 6.27.0, an input validation issue may have allowed staff users to access local files outside the intended data storage directories on the server. This issue is fixed in version 6.27.0.	3.8	More Details
CVE-2026-105130	LaraDashboard from 1.4.0 before 1.4.8 contains a race condition vulnerability in RegisterController::register that allows unauthenticated attackers to bypass the per-IP daily registration limit. Attackers can send many concurrent registration requests from one IP so all pass RegistrationGuardService::hasExceededIpLimit before recordRegistration runs, creating accounts in bulk and defeating anti-automation controls.	3.7	More Details
CVE-2026-103436	apcupsd through 3.14.14 discloses uninitialized stack memory in getupsvar() in src/cgi/upsfetch.c (used by upsstats.cgi, multimon.cgi, and upsstats.cgi. On the single-field path, when the matched STATUS line has fewer than three whitespace-separated tokens, sscanf("%*s %*s %s", answer) performs no assignment but the function returns success, and thus the caller prints the uninitialized destination buffer into the HTTP response.	3.7	More Details
CVE-2026-21833	HCL AION is affected by a vulnerability in which the Content-Security-Policy (CSP) HTTP response header is not configured. CSP helps prevent attacks such as Cross-Site Scripting (XSS) by restricting the sources from which scripts, styles, and other resources can be loaded. The absence of this header may reduce the effectiveness of browser-based security controls, potentially resulting in unintended behavior or negative security impacts under certain conditions.	3.7	More Details
CVE-2026-105125	LaraDashboard before 1.4.8 contains a path traversal vulnerability that allows unauthenticated attackers to read JSON files by manipulating the {lang} route segment. On Windows hosts, attackers can send URL-encoded backslash sequences like ..%5C to escape resources/lang and read composer.json or other application JSON files.	3.7	More Details
CVE-	Deployment of wrong handler vulnerability in Apache HTTP Server allows the target of some internal		

2026-42356	redirects from CGI programs to also be treated as CGI and executed. The target must already be in a directory enabled for CGI and have no other extension understood by mod_mime. This issue affects Apache HTTP Server: from 2.4.60 through 2.4.68.	3.7	More Details
CVE-2026-39601	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in WPdevelop Booking Calendar booking allows Leveraging Race Conditions.This issue affects Booking Calendar: from n/a through 11.8.4.	3.7	More Details
CVE-2026-67172	HCL BigFix Service Management is affected by an Information Disclosure vulnerability the application returns sensitive information in error messages when invalid inputs are sent to certain API endpoints . This information could enable an attacker to facilitate further attacks.	3.7	More Details
CVE-2026-104436	Zebra before 4.5.0 contains an uncontrolled resource consumption vulnerability that allows remote P2P peers to exhaust blocking-pool threads by sending oversized block locator vectors. Attackers can send getblocks or getheaders messages with up to 65,535 locator hashes, triggering per-hash chain lookups that degrade block validation, RPC, and mempool performance.	3.7	More Details
CVE-2026-105156	A weakness has been identified in YzmCMS up to 7.6. Impacted is the function Password of the file /common/function/system.func.php of the component MD5 Handler. Executing a manipulation of the argument pass can lead to password hash with insufficient computational effort. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is considered difficult. The exploit has been made available to the public and could be used for attacks. The vendor kindly explains: "Our regular release cycle is about 6 months. The last release was in the previous month, and our next scheduled version will be released in March 2027. We will implement the backward-compatible gradual hash migration feature in this upcoming release. (...) Before the new version is available, we will publish security mitigation guidance on our official documentation for existing deployers to reduce the risk."	3.7	More Details
CVE-2026-86834	The MetForm WordPress plugin before 4.3.1 does not properly restrict access to a debug file it writes to the web root on every form submission when its HubSpot Forms integration is enabled, allowing unauthenticated attackers to read upstream API response data, including correlation identifiers and cookies.	3.7	More Details
CVE-2026-105245	A vulnerability has been found in sgl-project sglang up to 0.5.21. This issue affects the function server_info of the file python/sglang/srt/entrypoints/http_server.py of the component HTTP Endpoint. Such manipulation of the argument api_key leads to cleartext transmission of sensitive information. It is possible to launch the attack remotely. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	3.7	More Details
CVE-2026-104424	Zebra before 6.1.0 contains an incorrect calculation vulnerability in its ZIP-317 block template selector that omits header and transaction-count size from the block budget. Attackers can place valid selectable transactions in a victim miner's mempool to shape templates into oversized blocks, causing rejection and wasted proof-of-work.	3.7	More Details
CVE-2026-80518	The WP Ultimate CSV Importer WordPress plugin before 9.2 does not use a site-specific secret when deriving the storage location of the import logs it writes under the uploads directory, nor does it block direct access to them, allowing unauthenticated attackers to retrieve the personal data of users imported from a CSV file.	3.7	More Details
CVE-2026-105237	A vulnerability was detected in linlinjava litemall up to 1.8.0. This affects an unknown part of the file litemall-admin-api/src/main/java/org/linlinjava/litemall/admin/web/AdminAuthController.java of the component Login Endpoint. The manipulation results in improper restriction of excessive authentication attempts. The attack may be performed from remote. A high complexity level is associated with this attack. It is indicated that the exploitability is difficult. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.7	More Details
CVE-2026-96962	The Pie Register WordPress plugin before 3.8.4.14 does not restrict access to an invitation-code report, allowing unauthenticated visitors who know a valid invitation code to obtain the username and email address of every user who registered with that code.	3.7	More Details
CVE-2026-105712	gpgtar in GnuPG before 2.5.19 can allow file overwrite via crafted data in an archive. When extracting an untrusted archive with --directory (aka -C) into an existing directory containing a pre-existing symlink, gpgtar can follow that symlink and create or overwrite a file outside the selected extraction directory. The write is limited by the extraction user's filesystem permissions. An archive extracted into a fresh empty directory does not have this risk.	3.6	More Details
	In Progress® Telerik® Fiddler® Classic for Windows, versions prior to v6.0.20262.10021, front-end request desynchronization is possible in the proxy request forwarding component. A request that		

CVE-2026-77803	contains both a Content-Length and a Transfer-Encoding header is forwarded with both headers present, while Fiddler frames the body using Transfer-Encoding only. The remaining bytes on the reused client connection are then parsed as a separate pipelined request, so a local threat actor with low privileges can cause a single malformed request to be split into two requests forwarded to the origin server and receive an additional smuggled response, without requiring a vulnerable server.	3.6	More Details
CVE-2026-105043	MathWorks Simulink before R2026b, when showing a crafted .slx file, can have blocks that are never visible in the Simulink Editor but will cause code execution.	3.6	More Details
CVE-2026-105289	A vulnerability was found in feelec-yishu feelcrm-os 1.0.0. Affected by this issue is the function htmlspecialchars_decode of the file App/Feelcrm/Common/Model/CrmDefineFormModel.class.php of the component Create Customer Endpoint. Performing a manipulation of the argument customer_form[remark] results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	3.5	More Details
CVE-2026-101887	BlueALSA (bluez-alsa/bluealsad) contains a division-by-zero vulnerability in the LC3plus sink decoder (a2dp-lc3plus.c, a2dp_lc3plus_dec_thread) that allows a Bluetooth-adjacent attacker to crash the daemon by sending a crafted RTP media header with an attacker-controlled frame count field set to zero. Attackers can establish an A2DP source connection with an LC3plus session negotiated against a victim running bluealsad as an A2DP sink and transmit a non-fragmented LC3plus media header with a zero frame count to trigger a SIGFPE in the decoding thread, causing a denial of service on builds compiled with LC3plus support enabled.	3.5	More Details
CVE-2026-103686	A flaw has been found in rhukster dom-sanitizer up to 1.0.15. Impacted is the function DOMSanitizer::isDangerousUrl of the file src/DOMSanitizer.php of the component URL Validation. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used. Upgrading to version 1.0.16 is recommended to address this issue. Patch name: 4623b565d060bc02ca5a07d8c8241fe28e2edfda. It is suggested to upgrade the affected component.	3.5	More Details
CVE-2026-80517	The WP Ultimate CSV Importer WordPress plugin before 9.2 does not properly validate the file types contained in an uploaded archive nor sanitise their content before storing them in a publicly served location, allowing high privilege users such as administrators to achieve Stored Cross-Site Scripting. On Multisite installations a site Administrator does not hold the unfiltered_html capability, so this lets them run scripts in the session of users who view the file, including Network Super Admins.	3.5	More Details
CVE-2026-104119	The Simple Shopping Cart WordPress plugin before 5.2.6 does not escape some of its settings field values before outputting them on an admin settings page, allowing high-privilege users such as administrators to perform Stored Cross-Site Scripting attacks, which is notably impactful on multisite installations where administrators do not have the unfiltered_html capability.	3.5	More Details
CVE-2026-105099	A weakness has been identified in Omega Solution CoinEx Crypto 2025. Affected by this vulnerability is an unknown functionality of the file /user/ticket of the component Ticket Attachment Upload. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The product web site does not exist anymore. Maybe the product got retired and/or replaced. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-82127	The Schema & Structured Data for WP & AMP WordPress plugin before 1.67 does not perform a capability check when saving several of its fields, nor escape them when outputting them back, allowing users with the editor role and above to inject arbitrary web scripts that execute when a higher privileged user views the affected screen. This is only exploitable on multisite installs, where editors do not hold the unfiltered_html capability.	3.5	More Details
CVE-2026-105173	A flaw has been found in code-projects Human Resource Management 1.0. This affects an unknown part of the file /humanresourcemanagementsystem/src/store/EventStore.php of the component Event Creation. Executing a manipulation of the argument eventSubject can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.	3.5	More Details
CVE-2026-105188	A vulnerability was found in code-projects Human Resource Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /views/admin/liveEventHistory.php of the component Live Event History. The manipulation of the argument eventSubject results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used.	3.5	More Details
CVE-2026-88791	The Safe Redirect Manager WordPress plugin before 2.3.0 does not properly validate the redirect destination when a wildcard redirect rule to an absolute URL is configured, allowing unauthenticated attackers to redirect visitors to an arbitrary external website via a crafted request path.	3.4	More Details

CVE-2026-104029	A flaw was found in SSSD. A local attacker can exploit this vulnerability by sending a specially crafted request to the autofs responder UNIX socket. Due to improper buffer offset calculation during request parsing, the service performs an out-of-bounds memory read. This flaw can cause the autofs responder process to crash, resulting in a denial of service (DoS).	3.3	More Details
CVE-2026-100270	In JetBrains YouTrack before 2026.2.19197 low-level Admin Read permission users could disclose integration credentials via import configurations	3.3	More Details
CVE-2026-58856	In returnOutputBufferLocked of DeprecatedCamera3StreamSplitter.cpp, there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-105767	Improper Neutralization of Special Elements used in an OS Command in the integrate-platform-docs composite GitHub Action of Chainguard Academy (edu) from commit 7375a80caabcc31c33ec90f29687ed78c13d16ff before commit fb0efb2537d326ab18c07d620875b8ed2a4b39f3 allows an actor who controls the project_id or storage_bucket inputs to execute arbitrary shell commands on the GitHub Actions runner, because the inputs are interpolated directly into Bash gcloud storage cp commands in several steps via \${ inputs.* } expressions. The only in-repository caller passed repository secrets and ran only on trusted triggers, so no untrusted input was known to reach the vulnerable steps.	3.3	More Details
CVE-2026-102138	An authenticated administrator on a node with an optional, separately licensed gateway role enabled could supply a connector URL that the server retrieved without sufficient validation of its scheme or destination, causing the server to issue requests to internal network services. Exploitation requires the licensed gateway role to be active.	3.3	More Details
CVE-2026-105766	Use of the backend-facing \$scheme variable in the trailing-slash directory redirect in nginx.conf of Chainguard Academy (edu) from commit 0b75ff98057f69b044a3e7194e428066ac5ad0d4 before commit 93dc0e50739c225f5aee2e803800a47fc0feb906 allows an on-path network attacker to read or modify documentation content served to a victim via an HTTPS request for a slashless directory path, because TLS terminates at the load balancer in front of Nginx and the resulting 301 response redirects the client to a plaintext http:// URL. Browsers that ship the HSTS preload list are not affected, because the .dev top-level domain is preloaded; clients that do not enforce HSTS, such as command-line HTTP clients and scripts that follow redirects, are affected.	3.1	More Details
CVE-2026-103680	A flaw was found in tnef. A heap-based buffer overflow can occur in the find_free_number() function when generating numbered backup suffixes for duplicate filenames. When numbered backups are enabled and file overwriting is disabled, an attacker can supply a specially crafted Transport Neutral Encapsulation Format (TNEF) file with an excessive number of colliding attachment filenames, causing the numeric counter to write past the allocated memory buffer. This issue may result in an application crash, leading to a Denial of Service (DoS), or potentially arbitrary code execution.	3.1	More Details
CVE-2026-105652	Ghost is a Node.js content management system. From 0.7.2 until 6.64.0, any staff-level user was able to determine the relative ordering of other staff users' hashed passwords. This does not directly disclose password hashes, and does not provide a practical path to recovering a password. This issue is fixed in version 6.64.0.	3.1	More Details
CVE-2026-66253	iControl is affected by a Session Timeout vulnerability, which could allow an attacker to exploit an unattended or abandoned active session, enabling unauthorized access to the application and the ability to perform actions on behalf of the victim.	3.1	More Details
CVE-2026-91023	The Motors WordPress plugin before 1.4.124 does not properly verify that a user is authorised to modify a listing before processing one of its listing management actions, allowing authenticated attackers with subscriber-level access and above to set metadata on posts they do not own, including overwriting product prices. Exploitation is possible only when WooCommerce is active and the Motors WordPress plugin before 1.4.124's paid featured-listing option is enabled, neither of which is a default configuration.	3.1	More Details
CVE-2026-105217	Cockpit CMS 2.12.0 before 2.14.1 disables TLS certificate verification in the cron.php web worker restart request, allowing network attackers to capture the worker token. Man-in-the-middle attackers on the outbound path to site_url can present any certificate to steal the worker/web/token value and start the web worker.	3.1	More Details
CVE-2026-87973	The If-So Dynamic Content WordPress plugin before 1.10.2 does not sanitize a conversion name before storing it, nor escape it when rendering the analytics page, allowing users with editor-level access to store JavaScript that executes in the session of a higher-privileged user who views that page.	3.1	More Details

CVE-2026-100280	In JetBrains YouTrack before 2026.2.19197 creating a project from an unreadable custom template was possible	3.1	More Details
CVE-2026-66248	iControl is affected by an Improper Error Handling vulnerability, which could allow an unauthenticated attacker to trigger verbose database and system errors, enabling the disclosure of sensitive internal infrastructure details used to plan advanced targeted attacks.	3.1	More Details
CVE-2026-102002	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.2.6 via the 'otter_form_widget_filter' parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the email addresses of the five most recent form submitters, their submission dates, and the site's total form submission count. The widget is registered whenever the themeisle_blocks_form_emails option is non-empty — the normal state after any Form block has been saved — meaning the exposure is active on any standard site using the plugin's form feature.	3.1	More Details
CVE-2026-104415	Ghost from 0.7.2 before 6.64.0 contains an information disclosure vulnerability in the Admin API that allows staff-level users to determine the relative ordering of other staff users' password hashes. Authenticated staff users can query the Admin API to infer hash ordering, though this does not directly reveal hashes or enable practical password recovery.	3.1	More Details
CVE-2026-66249	iControl is affected by a Missing Secure Attribute vulnerability, which could allow an attacker to intercept cookies transmitted over unencrypted HTTP connections, enabling the unauthorized extraction of sensitive information such as session identifiers.	3.1	More Details
CVE-2026-105164	A flaw has been found in NASA cFS up to 7.0.1. This issue affects the function CFE_FS_ParseInputFileNameEx of the file cfe/modules/fs/fsw/src/cfe_fs_api.c. This manipulation causes out-of-bounds read. Remote exploitation of the attack is possible. The pull request to fix this issue awaits acceptance.	2.7	More Details
CVE-2026-102844	A weakness has been identified in gedelumbung HospitalManagement up to c2d45543789a3887067d3915f69d44cfc2cf76a8. This vulnerability affects the function detail of the file application/modules/admin/controllers/laporan_data_pasien.php. Executing a manipulation of the argument id_param can lead to authorization bypass. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2.7	More Details
CVE-2026-105179	A weakness has been identified in SourceCodester Drug Recommendation System 1.0. This affects an unknown function of the file Admin/add_user.php of the component Password Handler. Executing a manipulation of the argument Password can lead to missing encryption of sensitive data. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	2.7	More Details
CVE-2026-100271	In JetBrains YouTrack before 2026.2.19197 missing authorisation on several endpoints allowed authenticated users to access information from other projects	2.7	More Details
CVE-2026-102583	A flaw was found in Moodle. An incorrect capability check in the artificial intelligence (AI) editor placement's image generation web service allows an authenticated user to invoke the feature without holding the required capability. This flaw permits unauthorized users to access and utilize the AI image generation functionality.	2.7	More Details
CVE-2026-27085	Shop manager Content Injection in Astra WordPress Theme <= 4.13.12 versions.	2.7	More Details
CVE-2026-102587	A flaw was found in Moodle. User list filters do not properly enforce visibility restrictions on user profile fields. An authorized user with manager privileges can filter user lists using profile attributes they are not permitted to view directly, resulting in unauthorized information disclosure by inferring hidden user data.	2.7	More Details
CVE-2026-94297	The Media Library Organizer WordPress plugin before 2.1.4 does not verify that the requesting user holds the target taxonomy's management capability before creating a new term, allowing users with contributor-level access and above to create publicly visible terms in any taxonomy registered on the site.	2.7	More Details
CVE-2026-	Ghost is a Node.js content management system. From 1.18.0 until 6.27.0, an SSRF vulnerability in the webhooks feature allowed staff users to probe internal hosts from the Ghost server. This issue is fixed	2.7	More

105682	in version 6.27.0.		Details
CVE-2026-103287	Ghost versions 1.18.0 before 6.27.0 contain a server-side request forgery vulnerability in the webhooks feature that allows staff users to probe internal hosts. Attackers with staff privileges can craft webhook requests to access internal network resources from the Ghost server.	2.7	More Details
CVE-2026-100264	In JetBrains YouTrack before 2026.2.18991 stored SMTP server credentials could be disclosed by changing the server host	2.7	More Details
CVE-2026-104994	Trivy before 0.71.0 allows directory traversal in Terraform filesystem functions when they try to access pathnames above the scan root. The risk occurs when using misconf scanning on untrusted input (e.g., upon a third-party pull request that contains a Terraform configuration), if sensitive data can be found at those unintended pathnames, and an adversary can then view a sensitive data value within scan output.	2.5	More Details
CVE-2026-105326	An argument injection flaw was found in CUPS. When email notification is configured, the CUPS scheduler accepts printer subscription requests that supply a mailto notify-recipient-uri. The mailto notifier passes the recipient address to the configured sendmail program without ensuring it cannot be interpreted as command-line options. A remote attacker who can reach the CUPS service could supply a crafted recipient value starting with "-" to influence sendmail behavior. Successful exploitation depends on the installed mail transfer agent and CUPS network exposure, and may lead to execution of attacker-controlled commands with the privileges of the CUPS service user.	2.5	More Details
CVE-2026-102582	A flaw was found in Moodle. The manual enrolment management page did not properly check whether the manual enrolment plugin was disabled, allowing users with enrolment permissions to access the page directly by navigating to its URL. Consequently, an authorized user could manage manual enrolments even after an administrator disabled the feature in the user interface.	2.2	More Details
CVE-2026-56599	HCL BigFix Service Management is affected by an Insecure Cookie Attribute Configuration vulnerability, which could allow an attacker to exploit missing security attributes such as SameSite, HttpOnly, Secure, and restrictive Paths, enabling Cross-Site Request Forgery (CSRF), session hijacking via Cross-Site Scripting (XSS), and unauthorized access.	2.2	More Details
CVE-2026-102580	A flaw was found in Moodle. An authenticated attacker can supply an improperly validated audience class name to the Report Builder component, allowing arbitrary class instantiation. This vulnerability enables the unauthorized creation of internal program objects, which may result in unexpected application behavior.	2.2	More Details
CVE-2026-103489	In JetBrains YouTrack before 2026.2.19422 hTML injection in VCS command failure notifications was possible	2.0	More Details
CVE-2026-105051	Denuvo Anti-Tamper through 2026-03-04 allows bypass of a hypervisor presence check via CPUID interception (SimpleSvm.sys on AMD; hyperkd.sys and hyperhv.dll on Intel).	1.9	More Details
CVE-2026-103442	External control of system or configuration setting vulnerability in The Wikimedia Foundation MediaWiki CentralAuth extension allows Code Injection. This issue affects MediaWiki CentralAuth extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-97305	Authorization Bypass Through User-Controlled Key vulnerability in Themeisle AI Chatbot for WordPress - Hyve Lite hyve-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AI Chatbot for WordPress - Hyve Lite: from n/a through 2.0.2.	N/A	More Details
CVE-2026-102509	Memory Allocation with Excessive Size Value, Allocation of Resources Without Limits, and Uncontrolled Recursion in the Java implementation of Apache PLC4X (PLC4J) allow a malicious or impersonated device to exhaust the memory or stack of the client application, causing a denial of service. In the OPC UA driver these defects are reachable before authentication: the offending data is parsed while the secure channel and session are being established, before the server's identity has been bound to it. Configuring a trusted server therefore does not prevent exploitation by an attacker who can impersonate it. The individual defects are: - Length-prefixed byte strings are allocated at the size claimed on the wire before the length is checked against the data actually received (0.10.0 through 0.13.1). - Array fields in generated protocol parsers pre-allocate a list with the element count claimed on the wire, allowing a single count field to trigger a multi-gigabyte allocation. This parser is shared by all PLC4J drivers; the OPC UA driver is the verified pre-authentication path (0.10.0 through 0.13.1). - The OPC UA driver accumulates message chunks without enforcing the negotiated maximum chunk count and message size (0.12.0 through 0.13.1). - The OPC UA driver pre-allocates collections using element counts received from the server (0.10.0 through 0.13.1). - Recursive protocol types are parsed without	N/A	More Details

	a nesting-depth limit. The same defect in the Go implementation is covered by CVE-2026-102510 https://cveprocess.apache.org/cve5/CVE-2026-102510 . This issue affects Apache PLC4X: from 0.10.0 before 1.0.0. Users are recommended to upgrade to version 1.0.0, which fixes the issue.		
CVE-2026-104966	Plane is an open-source project management tool. Prior to 1.4.0, two endpoint families fail to verify that nested resource identifiers belong to the workspace and project named in the URL. An authenticated user can read or modify estimates from another workspace through PATCH <code>/api/workspaces/{slug}/projects/{project_id}/estimates/{estimate_id}/</code> , and can inject comments into an issue from another workspace through POST <code>/api/workspaces/{slug}/projects/{project_id}/issues/{issue_id}/comments/</code> . ProjectEntityPermission verifies membership in the workspace and project from the URL, but estimate_id and issue_id are fetched by primary key without confirming the same scope. The list, retrieve, and destroy handlers correctly scope their queries, demonstrating the inconsistency. This issue is fixed in 1.4.0.	N/A	More Details
CVE-2026-102779	Joomla Extension - joomlafry.com - Unauthenticated forced execution of published automation tasks in TF Content 2.9.0 - 2.9.4 - The extension exposes the site task <code>`records.custom_action`</code> without authentication, ACL, CSRF, task-trigger, content-binding, or cron-token enforcement. A Guest can supply the numeric ID of any published TF Content task and make the component dispatch its configured executor immediately.	N/A	More Details
CVE-2026-104968	Plane is an open-source project management tool. Prior to 1.4.0, GET <code>/api/workspaces/{slug}/entity-search/?query_type=user_mention</code> returns workspace-member display names, UUIDs, and avatar URLs to any authenticated user who knows the workspace slug, even when the caller is not a workspace member. The endpoint also exposes ProjectMember rows under the same condition. SearchEndpoint in <code>apps/api/plane/app/views/search/base.py</code> inherits BaseAPIView with only <code>permission_classes = [IsAuthenticated]</code> and performs no workspace-membership check. This issue is fixed in 1.4.0.	N/A	More Details
CVE-2026-92872	Pgpool-II inserts sensitive information into log file, which may allow an authenticated attacker to obtain the cluster information.	N/A	More Details
CVE-2026-102777	Joomla Extension - svenbluege.de - Server-side request forgery in the Google Photos picker in Event Gallery extension < 6.6.0 - The Google Photos picker of the back-end upload page fetches the thumbnails of the picked images through the server, with the OAuth access token of the Google Photos account. The task took the address to fetch from the request without checking it and asked for no form token. A prepared page on another web site could therefore make the server send the access token of the account to any address, or fetch addresses inside the server's network, in the name of a logged in administrator; a back-end user with the permission "Manage" could do the same directly. The token is valid for about an hour and reaches what the picker session of the account reaches.	N/A	More Details
CVE-2026-97309	Missing Authorization vulnerability in Webful Creations RepairBuddy computer-repair-shop allows Retrieve Embedded Sensitive Data.This issue affects RepairBuddy: from n/a through 4.1226.	N/A	More Details
CVE-2026-86671	In Eclipse Che versions 7.29.0 and later, the GET <code>`/api/scm/resolve`</code> and <code>`POST /api/factory/resolver`</code> endpoints pass an attacker-controlled URL to <code>`URLFetcher.fetch()`</code> , which calls <code>`new URL(url).openConnection()`</code> with no scheme or host allow-list and returns the response body to the caller. Any authenticated Che user can read arbitrary local files via the <code>file://</code> scheme (including the pod's Kubernetes service-account token at <code>`file:///var/run/secrets/kubernetes.io/serviceaccount/token`</code>), reach internal HTTP services and cloud instance metadata endpoints (169.254.169.254), and have their stored SCM personal access token attached as an <code>`Authorization`</code> header to a host of their choosing. The same credential-forwarding behavior also fires when a victim opens a workspace from a malicious devfile whose <code>`parent.uri`</code> points to an attacker-controlled server, enabling exfiltration of the victim's SCM PAT without direct API access. No fix is available.	N/A	More Details
CVE-2026-93460	A stored cross-site scripting vulnerability via appended strings in email form fields exists in baserCMS. If this vulnerability is exploited, an arbitrary script may be executed in the user's web browser.	N/A	More Details
CVE-2026-51936	Zetetic SQLCipher before 4.15.0 allows SQL injection. The <code>sqlcipher_export</code> convenience function can be used to copy the contents of one attached database into another. It is most often used to convert between plaintext and encrypted databases. It needs to do dynamic schema manipulation, and thus the function temporarily clears defensive restrictions during operation. A vulnerability in the handling of the source database name parameter made it possible for a caller to supply a crafted source name, which could execute statements that defensive mode would otherwise block. This could allow direct modifications to the <code>sqlite_schema</code> table and database corruption. SQLCipher 4.15.0 now strictly validates the source database name and prevents the bypass.	N/A	More Details
	Langflow is a tool for building and deploying AI-powered agents and workflows. From 1.6.8 until 1.9.1,		

CVE-2026-105699	Langflow authenticated access to the project identifier in a project-scoped MCP connection but did not authorize the resource URI supplied to resources/read. read_resource forwarded the attacker-controlled URI to handle_read_resource, which parsed a flow_id and filename and called storage_service.get_file without verifying that the flow belonged to the authenticated user or current project. A user with access to any project-scoped MCP endpoint could therefore request another user's flow-backed file, while global handle_list_resources and handle_list_tools behavior could disclose flow and file identifiers that made targeting easier. The vulnerability disclosed uploaded documents, structured data, prompts, and other private flow artifacts across tenants but did not modify victim files or stored flows. This issue is fixed in version 1.9.1.	N/A	More Details
CVE-2026-92873	Pgpool-II contains an incorrect implementation of an authentication algorithm, which may allow an unauthenticated attacker to promote an arbitrary watchdog node to the leader node.	N/A	More Details
CVE-2026-103335	Insertion of Sensitive Information Into Sent Data vulnerability in Deepen Bajracharya Video Conferencing with Zoom video-conferencing-with-zoom-api allows Retrieve Embedded Sensitive Data.This issue affects Video Conferencing with Zoom: from n/a through 4.6.10.	N/A	More Details
CVE-2026-86101	An improper authorization vulnerability in WatchGuard Fireware OS's SAML login process allows a remote, authenticated SAML user with access only to the Access Portal to obtain unauthorized Mobile VPN with SSL access through a specially crafted request.	N/A	More Details
CVE-2026-92868	An improper certificate validation vulnerability exists in Pgpool-II, which may allow an unauthenticated attacker to bypass client certificate authentication.	N/A	More Details
CVE-2026-93462	A missing authentication for critical function vulnerability exists in baserCMS. If this vulnerability is exploited, a remote attacker may obtain sensitive information.	N/A	More Details
CVE-2026-18145	A stack-based buffer overflow vulnerability in the spamBlocker (spamd) service of WatchGuard Fireware OS allows an authenticated attacker with administrator privileges to crash the service or potentially execute arbitrary code by sending a specially crafted management request.	N/A	More Details
CVE-2026-94201	Ash stores :atom-typed attributes as strings and compares them as strings. When such an attribute is referenced in a filter, the comparison value is coerced through Ash.Type.Atom. Because the type defined no coerce/2 callback, coercion fell back to the default (cast_input/2), which calls String.to_atom/1 when the attribute is configured with the unsafe_to_atom?: true constraint. Filtering such an attribute with attacker-controlled strings therefore interned a new, permanent atom for every distinct value. Atoms are never garbage collected and the BEAM caps the atom table, so an actor who can supply filter values for a public, filterable :atom attribute declared with unsafe_to_atom?: true can exhaust the atom table and crash the node (denial of service). AshPaperTrail is a notable example: its version resources expose a public, filterable version_action_name atom attribute with unsafe_to_atom?: true by default. The fix adds a coerce/2 to Ash.Type.Atom that never interns atoms — a comparison value is left as a string, since the type is stored and compared as a string. Setting the attribute from action input (cast_input/2, which still honors unsafe_to_atom?) is unchanged. This issue affects ash: from 3.5.1 before 3.34.3.	N/A	More Details
CVE-2026-18105	An uncontrolled resource consumption vulnerability in Fireware OS's diagnostic tasks feature allows a low-privileged, authenticated user to cause a denial of service of the system's diagnostic tools by repeatedly starting and aborting a specially crafted diagnostic task through the web UI.	N/A	More Details
CVE-2026-13224	A path traversal vulnerability in the Fireware OS WebUI management agent allows an authenticated administrator to read or list arbitrary files on the local filesystem by sending a specially crafted management request.	N/A	More Details
CVE-2026-103510	P4 Search prior to 2026.4.2 does not fail securely when its service authentication token is blank. In affected configurations, an unauthenticated attacker with network access can obtain the highest application privilege, potentially leading to compromise of P4 Search and the connected P4 Server.	N/A	More Details
CVE-2026-13046	A deserialization of untrusted data vulnerability in WatchGuard Fireware OS's SAML single sign-on session handling (samId) allows an attacker who has already obtained the ability to write files on the appliance to execute arbitrary code in the context of the samId service by causing samId to load a maliciously crafted session file.	N/A	More Details
CVE-2026-103470	In Internet2 Grouper before 7.5.1 (in some configurations), a user who is allowed to create or edit rules in the User Interface can escalate privileges.	N/A	More Details

CVE-2026-97070	Authorization Bypass Through User-Controlled Key vulnerability in CozyThemes Cozy Blocks cozy-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Cozy Blocks: from n/a through 2.2.23.	N/A	More Details
CVE-2026-81433	A stack-based buffer overflow vulnerability in WatchGuard Fireware OS's DHCP fingerprinting daemon (fingerd) allows an unauthenticated attacker with adjacent network access to execute arbitrary code or crash the process by sending a specially crafted DHCP packet.	N/A	More Details
CVE-2026-92869	An out-of-bounds write vulnerability exists in Pgpool-II, which may allow an authenticated attacker to cause abnormal process termination.	N/A	More Details
CVE-2026-103511	Perforce P4 Search prior to 2026.4.2 does not validate file names supplied to its extension installation feature. An attacker with super-user or service-token privileges can write files with arbitrary content to the P4 Search installation directory.	N/A	More Details
CVE-2026-103512	Perforce P4 Search prior to 2026.4.2 trusts a client-supplied address when validating certain authentication requests. An attacker holding a stolen P4 Server ticket can bypass host-based ticket restrictions and trusted-address controls, gaining access to P4 Search as the ticket's owner.	N/A	More Details
CVE-2026-93463	A cross-site scripting vulnerability via script validation bypass exists in baserCMS. If this vulnerability is exploited, an arbitrary script may be executed in the user's web browser.	N/A	More Details
CVE-2026-103441	Deserialization of untrusted data vulnerability in The Wikimedia Foundation MediaWiki Wikibase extension allows Leverage Executable Code in Non-Executable Files. This issue affects MediaWiki Wikibase extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-93464	A stored cross-site scripting vulnerability via custom content descriptions exists in baserCMS. If this vulnerability is exploited, an arbitrary script may be executed in the user's web browser.	N/A	More Details
CVE-2026-103507	Perforce P4 Search prior to 2026.4.2 does not restrict file paths written through its logging configuration interface. An attacker holding the service authentication token can write arbitrary files on the host, potentially leading to code execution as the P4 Search service account.	N/A	More Details
CVE-2026-97150	When converting baserCMS4-style addons to baserCMS5-style ones, BcAddonMigrator includes "config.php" from the addon, which means the PHP code in the file is executed. Arbitrary files on the system may be read or deleted by an administrative user.	N/A	More Details
CVE-2026-92871	A NULL pointer dereference vulnerability exists in Pgpool-II, which may allow an unauthenticated attacker to cause abnormal termination of the watchdog process.	N/A	More Details
CVE-2026-92870	A stack-based buffer overflow vulnerability exists in Pgpool-II, which may allow an unauthenticated attacker to cause abnormal process termination.	N/A	More Details
CVE-2026-102775	Joomla Extension - phoca.cz - Authorisation bypass through user-controlled key (IDOR) in Order View in Phoca Cart 5.0.0 - 6.1.8 - Phoca Cart's order-file download endpoint does not verify the download tokens it asks for. The d (download token) and o (order token) parameters are checked for non-emptiness only — they are never compared to the stored download_token / order_token values. As a result, any remote user (including a guest with no account at all) can download any customer's digital goods by enumerating sequential id values and supplying arbitrary non-empty tokens.	N/A	More Details
CVE-2026-104892	Plane is an open-source project management tool. Prior to 1.4.0, aPITokenLogMiddleware logs API keys in plaintext. This allows someone with low privileges to steal user API keys and further escalate their privileges. This issue is fixed in 1.4.0.	N/A	More Details
CVE-2026-93317	An unauthenticated attacker controlling a registry or OCI-layout blob source could provide blob contents that did not match the claimed digest. The resulting snapshot could be cached under that digest and reused by a later victim build, compromising build-input integrity.	N/A	More Details
CVE-2026-103321	MISP contains a stored cross-site script (XSS) vulnerability in the event graph preview feature. The event graph preview image field was accepted and stored without server-side validation. On the client side, the stored value was rendered into an HTML img element's src attribute via string concatenation, allowing a crafted value to break out of the attribute context and inject arbitrary script. Preconditions: - An authenticated MISP user with the ability to create or modify an event graph entry. - A second user (the victim) who views the event graph and triggers the preview popover. Impact: - Execution of arbitrary JavaScript in the victim's browser within the MISP application context. - Potential theft of	N/A	More Details

	session tokens, cookies, or sensitive data accessible to the victim's browser. - Potential for performing actions on behalf of the victim within the MISP application. Affected: MISP versions prior to the fix (commit applied after v2.5.48).		
CVE-2026-97259	Authorization Bypass Through User-Controlled Key vulnerability in WP Hosting AS Pay with Vipps for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Pay with Vipps for WooCommerce: from n/a through 6.2.4.	N/A	More Details
CVE-2026-94545	Satori is a library to convert HTML and CSS to SVG. Starting in version 0.0.27 and prior to version 0.33.5, Satori does not properly escape certain values before including them in generated SVG output. This can allow crafted values to be interpreted as SVG markup. The impact depends on how the generated SVG is consumed. Version 0.33.5 contains a patch. No complete workaround exists besides upgrading. Applications that cannot immediately upgrade should not render attacker-controlled content with Satori.	N/A	More Details
CVE-2026-103389	MISP contains a stored cross-site scripting (XSS) vulnerability in the galaxy icon handling path. The icon field of a galaxy object was persisted without any server-side validation through the galaxy add, edit, and sync/import capture endpoints. The stored value was subsequently concatenated directly into HTML markup by the D3-based correlation graph rendering scripts (both the default and Overmind themes) using the .html() method. A user holding the perm_galaxy_editor permission, which is granted to the stock User role, could store arbitrary HTML or JavaScript in the icon field. Any other user who opened the correlation graph of an event containing a cluster belonging to that galaxy would have the injected script executed in their browser session. Impact: - Arbitrary script execution in the context of the victim's MISP session - Potential theft of session credentials, manipulation of displayed data, or initiation of actions on behalf of the victim - Affects both the default and Overmind UI themes Affected versions: <2.5.48	N/A	More Details
CVE-2026-19395	In Qt for MCUs, a Text element that displays styled text halts the device if an tag in the text contains an attribute with an empty value. The text parser passes the empty value to an internal check that only accepts non-empty values. The check fails and reports an error, and the default error handler halts the device.	N/A	More Details
CVE-2026-59782	The JavaScript preprocessing (Duktape) engine on Zabbix server has a vulnerability where a limited administrator is able to read raw heap data potentially resulting in leaked data from other running preprocessors not available to said administrator.	N/A	More Details
CVE-2026-59783	The Zabbix Server/Proxy has a vulnerability where binary items can crash the Server/Proxy on certain NULL byte input leading to potential loss of availability. This only affects deployments where MySQL/MariaDB database is used as the Zabbix database.	N/A	More Details
CVE-2026-59785	Host search in Frontend allows filtering by fields that are not displayed, including stored IPMI and PSK credentials. A user with read access can guess a credential and see from the search result whether the guess was right, letting them uncover it.	N/A	More Details
CVE-2026-59786	Zabbix Server and Proxy accept the active agent heartbeat message regardless of the configured PSK or certificate authentication. This means someone with access to the Zabbix trapper port can report an arbitrary host using an active agent as available, resulting in a loss of integrity.	N/A	More Details
CVE-2026-102508	Improper Verification of Cryptographic Signature and Improper Certificate Validation in the OPC UA driver of Apache PLC4X (PLC4J) allows an attacker in a network position between client and server to impersonate the OPC UA server and to read, forge or modify secure-channel traffic, including user credential ssent by the client. The defect manifests differently depending on the version: - In 0.9.0 through 0.11.0 a failed message-signature check is only logged and never enforced, and there is no mechanism to verify the server certificate: it is taken from the unauthenticated GetEndpoints discovery response and used to encrypt the user's password. - In 0.12.0 through 0.13.1 the signature check is inverted (valid signatures are rejected, invalid ones accepted), and server certificates are accepted without a trust anchor by default. - In all affected versions the default security policy is None. Starting with 0.12.0 the driver additionally continues silently at a weaker security policy than the one configured, and starting with 0.13.0 endpoint selection prefers the weakest matching endpoint. Users checking only for one of these mechanisms may wrongly conclude they are unaffected. This issue affects Apache PLC4X: from 0.9.0 before 1.0.0. Users are recommended to upgrade to version 1.0.0, which fixes the issue. Version 1.0.0 verifies message signatures correctly, refuses to connect unless the server certificate can be verified against a configured trust store or pinned certificate, defaults to Basic256Sha256 with SignAndEncrypt, and fails the connection if the negotiated security policy is weaker than the configured one.	N/A	More Details
CVE-2026-59787	The Perl SNMP trap receiver script shipped with Zabbix does not properly neutralize the ZBXTRAP record delimiter in trap content. This means someone able to send SNMP traps can inject a record targeting another host, resulting in a loss of integrity.	N/A	More Details

CVE-2026-59788	The email media type OAuth form passes the Authorization endpoint value to window.open() without validating the URL scheme, so a javascript: URL is executed in the browser. This means a crafted media type configuration, deliverable as an import file, runs arbitrary JavaScript as the Super Admin who grants consent.	N/A	More Details
CVE-2026-93316	If BuildKit daemon is started with --cdi-disabled it can lead to daemon panic when builds try to use CDI devices. This can happen maliciously or by accident.	N/A	More Details
CVE-2026-93318	A malicious image can advertise DiffIDs from another image while containing different layer contents. In affected versions, BuildKit could use the advertised DiffIDs to derive cache and snapshot identity without validating that they matched the actual layer contents. If a BuildKit daemon with shared or persistent cache first processes such a malicious image, a later build using the victim image may mount the attacker-controlled layer contents as the base image. This can allow code from the malicious image to run in the victim build, for example by replacing a commonly executed path such as /bin/sh. The attacker-controlled code may read build secrets mounted into the build, access other build resources, alter output artifacts, or hang the build. The issue affects both regular snapshotters and lazy-pulling snapshotters such as stargz.	N/A	More Details
CVE-2026-103087	Uncontrolled recursion in the Gosub browser engine (gosub-engine) through 0.1.0 and main before commit 46868b3 allows a remote attacker to cause a Denial of Service (stack exhaustion and application crash) via an SVG document containing an excessive number of deeply nested elements. Because the engine does not limit the nesting depth of processed SVG nodes, rendering such a document overflows the thread stack and terminates the application. The malicious SVG can be embedded through the SRC attribute of an IMG element, and thus exploitation only requires the victim to visit an attacker-controlled web page.	N/A	More Details
CVE-2026-96342	Missing Authorization vulnerability in Amauri.IO WPMobile.App wpappninja allows Retrieve Embedded Sensitive Data.This issue affects WPMobile.App: from n/a through 11.83.	N/A	More Details
CVE-2026-103012	Claude Code selected an API key stored by Claude Code, for example from an earlier `/login` or written directly to its configuration, ahead of the user's valid Claude Enterprise or Team sign-in when fetching the organization's server-managed settings, even though the session itself authenticated with the Enterprise or Team account. When the settings endpoint rejected that stored key, the session started without the organization's server-managed policy (such as permission deny rules, model restrictions and managed-only locks) or, if a previously cached copy existed on the machine, kept applying that stale copy without receiving later policy changes — while continuing to operate as the organization's account. Triggering this required local access to a device with such a stored API key; the no-policy case additionally required that no managed settings had previously been cached. Endpoint-managed (MDM or file-based) settings were not affected. Claude for Enterprise organizations were affected from version 2.0.68; Claude for Work (Team) organizations from version 2.1.38, when server-managed settings became available to them. Users on standard Claude Code auto-update have received this fix already. Users performing manual updates are advised to update to version 2.1.260 or later. Thank you to Tamas Voros / NVIDIA AI Red Team for reporting this issue.	N/A	More Details
CVE-2026-10726	Cato Windows SDP Client before version 6.12.6 contains an arbitrary file disclosure vulnerability. A low-privileged local user can cause the Windows service, running as Local System, to read and disclose arbitrary local files due to improper file path validation and missing TLS certificate enforcement.	N/A	More Details
CVE-2026-10739	Cato Networks SDP Client for Windows before 6.12.6 allows a local user to delete arbitrary files with SYSTEM privileges via improper validation of a client-supplied SID over a local IPC named pipe.	N/A	More Details
CVE-2026-93319	A malicious external BuildKit frontend can send requests using the internal API that can create conditions for a data race that can cause the BuildKit daemon to panic.	N/A	More Details
CVE-2026-63266	LibreOffice Calc can link a cell range to an external data source, and the link is saved in the document. Through such a link a document could open an embedded Firebird database that wrote a file to any location the user could write to. In fixed versions an embedded Firebird database can open or create files only inside its own private directory.	N/A	More Details
CVE-2026-63267	LibreOffice Calc can link a cell range to an external csv data source, and the link is saved in the document. Such a link was fetched while the document loaded, so opening a document could read a local file into the sheet, or make a request to a host of the document's choosing. In fixed versions external data links are updated under the same link update control as other links in a spreadsheet.	N/A	More Details
CVE-	LibreOffice Calc can link a cell range to an external data source, and the link is saved in the document.		

2026-63268	A link of the sql type could name a folder of local text files as a database, so opening a document could read a local text file into the sheet. In fixed versions only the csv, html and xml data providers are restored when a document is loaded.	N/A	More Details
CVE-2026-63269	LibreOffice can link to audio and video files from a document, and on Linux it plays them with GStreamer. A linked media file could be an HLS playlist that made GStreamer read the local files and remote URLs it listed while the document loaded, and their contents could end up in the document. In fixed versions LibreOffice does not follow playlists that name further resources, and linked media is under link update control.	N/A	More Details
CVE-2026-63270	URLs could be constructed which expanded environment variable or INI file values, so potentially sensitive information could be exfiltrated to a remote server on opening a document containing such links. The check added for CVE-2024-12426 did not cover every place a document can supply a URL. XForms instance data and the Calc csv and sql data providers still reached the expansion. In fixed versions these places refuse URLs with internal schemes when the URL comes from the document.	N/A	More Details
CVE-2026-63277	LibreOffice Calc can link a cell range to an external data source, and the link is saved in the document. A document could name a Java database driver for such a link to be loaded from a remote location, so opening the document could run Java code from that location. In fixed versions an entry in a Java class path has to be a file URL.	N/A	More Details
CVE-2026-93320	BuildKit may be tricked into performing file actions with special file inodes where regular files are expected. Special files may block operations or, on rootful workers, allow unintended host device access.	N/A	More Details
CVE-2026-93323	The Dockerfile frontend loaded the Dockerfile and .dockerignore files of a build context into memory without a size limit. A build context containing an oversized file could make buildkitd allocate memory proportional to that file, potentially exhausting memory and terminating the daemon, which interrupts other builds on the same instance. Fixed by rejecting such files above 16 MiB.	N/A	More Details
CVE-2026-105632	Plane is an open-source project management tool. Prior to 1.4.0, the GraphQL joinProject mutation lets any workspace member add themselves to any project in that workspace including network=0 (secret/private) projects they were never invited to and grants them a full Member role (read + write). The resolver checks only workspace-level membership/role and never checks the target project's visibility (network). This collapses project-level tenant isolation within a workspace: a low-privilege member can read and modify confidential data in every private project. This issue is fixed in 1.4.0.	N/A	More Details
CVE-2026-103388	MISP renders the source field of a Galaxy Cluster as a clickable hyperlink whenever the stored value passes PHP's FILTER_VALIDATE_URL validation. Because FILTER_VALIDATE_URL accepts the javascript: URI scheme, a user with galaxy editor privileges on the local instance or on a synced instance could store a javascript: URL as the cluster source. When another user views the affected Galaxy Cluster and clicks the rendered link, the embedded script executes in the victim's browser context, enabling session hijacking, data exfiltration, or actions performed on behalf of the victim. Preconditions: - Attacker must hold galaxy editor privileges (local or via sync). - Victim must view the affected cluster and click the malicious link. Impact: - Stored cross-site scripting (XSS) in the victim's browser. - Potential session theft, credential harvesting, or unauthorized actions within the MISP application. Affected: <2.5.48.	N/A	More Details
CVE-2026-91860	A prototype pollution vulnerability exists in the deep merge helpers of Vaadin Charts and Vaadin Component Base. Merging an object the application does not control into a chart configuration or into a component's i18n property writes onto Object.prototype, making the injected properties visible to every object in the running application. Users of affected versions should apply the following mitigation or upgrade. Releases that have fixed this issue include: Product version Vaadin 23.0.0 - 23.6.13 Vaadin 24.0.0 - 24.9.20 Vaadin 24.10.0 - 24.10.9 Vaadin 25.0.0 - 25.1.11 Vaadin 25.2.0 - 25.2.6 Mitigation Upgrade to 23.6.14 Upgrade to 24.9.21 Upgrade to 24.10.10 Upgrade to 25.1.12 Upgrade to 25.2.7 or newer Please note that Vaadin versions 10-13 and 15-22 are no longer supported and you should update either to the latest 23, 24, 25 version. Artifacts Maven coordinates Vulnerable versions Fixed version com.vaadin:vaadin 23.0.0 - 23.6.13 >=23.6.14 com.vaadin:vaadin 24.0.0 - 24.9.20 >=24.9.21 com.vaadin:vaadin 24.10.0 - 24.10.9 >=24.10.10 com.vaadin:vaadin 25.0.0 - 25.1.11 >=25.1.12 com.vaadin:vaadin 25.2.0 - 25.2.6 >=25.2.7 com.vaadin:vaadin-core 24.7.0 - 24.9.20 >=24.9.21 com.vaadin:vaadin-core 24.10.0 - 24.10.9 >=24.10.10 com.vaadin:vaadin-core 25.0.0 - 25.1.11 >=25.1.12 com.vaadin:vaadin-core 25.2.0 - 25.2.6 >=25.2.7 com.vaadin:vaadin-charts-flow 23.0.0 - 23.6.13 >=23.6.14 com.vaadin:vaadin-charts-flow 24.0.0 - 24.9.20 >=24.9.21 com.vaadin:vaadin-charts-flow 24.10.0 - 24.10.9 >=24.10.10 com.vaadin:vaadin-charts-flow 25.0.0 - 25.1.11 >=25.1.12 com.vaadin:vaadin-charts-flow 25.2.0 - 25.2.6 >=25.2.7 npm packages npm package Vulnerable versions Fixed version @vaadin/charts 23.0.0 - 23.6.4 >=23.6.5 @vaadin/charts 24.0.0 - 24.9.17 >=24.9.18 @vaadin/charts 24.10.0 - 24.10.4 >=24.10.5 @vaadin/charts 25.0.0 - 25.1.11 >=25.1.12 @vaadin/charts 25.2.0 - 25.2.8 >=25.2.9 @vaadin/component-base 24.7.0 - 24.9.17 >=24.9.18 @vaadin/component-base 24.10.0 - 24.10.4 >=24.10.5 @vaadin/component-base 25.0.0 - 25.1.11	N/A	More Details

	>=25.1.12 @vaadin/component-base 25.2.0 - 25.2.8 >=25.2.9		
CVE-2026-104809	DigitalCanion has discovered a vulnerability that allows an attacker to cause the system to load an attacker-controlled .so file instead of the expected legitimate module. The loading mechanism relies on a predictable module name without adequately verifying the file's origin or integrity. A malicious shared object using the expected name can therefore be loaded by a privileged process. The module code then executes within the context and privileges of that process. This results in arbitrary code execution and full compromise of the Mitel Linux virtual machine.	N/A	More Details
CVE-2026-93547	A missing authorization check in the Vaadin Spreadsheet component allows an authenticated user of an application that renders a spreadsheet to add or replace cell comments on a sheet that has protection enabled, including on cells that are locked. Writing a comment to a cell that does not exist yet also creates the row and the cell. Users of affected versions should apply the following mitigation or upgrade. Releases that have fixed this issue include: Product version Vaadin 23.1.0 - 23.6.13 Vaadin 24.0.0 - 24.9.21 Vaadin 24.10.0 - 24.10.9 Vaadin 25.0.0 - 25.1.11 Vaadin 25.2.0 - 25.2.6 Vaadin Framework 7 and 8 with the Spreadsheet add-on 2.0.0 - 3.1.0 Mitigation Upgrade to 23.6.14 Upgrade to 24.9.22 Upgrade to 24.10.10 Upgrade to 25.1.12 Upgrade to 25.2.7 or newer Upgrade the Spreadsheet add-on to 3.1.1 Please note that Vaadin versions 10-13 and 15-22 are no longer supported and you should update either to the latest 23, 24, 25 version. Artifacts Maven coordinates Vulnerable versions Fixed version com.vaadin:vaadin 23.1.0 - 23.6.13 >=23.6.14 com.vaadin:vaadin 24.0.0 - 24.9.21 >=24.9.22 com.vaadin:vaadin 24.10.0 - 24.10.9 >=24.10.10 com.vaadin:vaadin 25.0.0 - 25.1.11 >=25.1.12 com.vaadin:vaadin 25.2.0 - 25.2.6 >=25.2.7 com.vaadin:vaadin-spreadsheet-flow 23.1.0 - 23.6.13 >=23.6.14 com.vaadin:vaadin-spreadsheet-flow 24.0.0 - 24.9.21 >=24.9.22 com.vaadin:vaadin-spreadsheet-flow 24.10.0 - 24.10.9 >=24.10.10 com.vaadin:vaadin-spreadsheet-flow 25.0.0 - 25.1.11 >=25.1.12 com.vaadin:vaadin-spreadsheet-flow 25.2.0 - 25.2.6 >=25.2.7 com.vaadin:vaadin-spreadsheet 2.0.0 - 3.1.0 >=3.1.1	N/A	More Details
CVE-2026-102780	Joomla Extension - joomlafry.com - Unauthenticated cross-record publication and mass assignment in TF Content 2.9.0 - 2.9.4 - The extension unconditionally authorizes both creation and editing in its public `RecordController`. Its shared frontend save controller accepts the raw `jform` array, assigns the request-selected existing record ID, and saves it without filtering submitted properties through the configured form. A Guest can obtain a valid token from Joomla's public login form and modify any TF Content row, including mass-assigning `published`, `access`, and `created_by`.	N/A	More Details
CVE-2026-92867	An out-of-bounds write vulnerability exists in Pgpool-II, which may allow an authenticated attacker to cause abnormal process termination or arbitrary code execution.	N/A	More Details
CVE-2026-104706	DigitalCanion has discovered a path traversal vulnerability that allows to view or download sensitive system files over the portal https://<ip>:8443 via menus Administration -> View Logs	N/A	More Details
CVE-2026-104805	DigitalCanion has discovered a vulnerability in the backup restoration functionality that allows an attacker with access to the configured backup repository to introduce arbitrary files into the system during restoration. The specific flaw exists within the backup restoration mechanism, which fails to properly validate the paths, file types, integrity, and authenticity of files contained within a restored TGZ archive. The application does not perform file-signature verification before extracting the archive, allowing a specially crafted backup to contain attacker-controlled files. An attacker with access to the backup SFTP or other configured repository can therefore provide a malicious TGZ archive that, when restored by the system, may place arbitrary files on the underlying Linux system. Depending on the location and permissions of the extracted files, this behavior can potentially be leveraged to achieve arbitrary code execution with root privileges and compromise the underlying virtual machine. The absence of enforced backup passwords further reduces the protection provided by the backup mechanism and may facilitate unauthorized access to the repository.	N/A	More Details
CVE-2026-104806	DigitalCanion has discovered a path traversal vulnerability that allows an attacker to access files outside of the intended directory. The specific flaw exists within the Maintenance → System Logs functionality of the web management portal listening on TCP port 443. The application fails to properly validate user-supplied file paths, allowing an attacker to manipulate the requested path and traverse the underlying directory structure. By exploiting this vulnerability, an attacker can access and download files located outside the intended system logs directory, including potentially sensitive system and application files.	N/A	More Details
	Integer Overflow, Improper Validation of Array Index, Uncontrolled Recursion and Memory Allocation with Excessive Size Value in the Go implementation of Apache PLC4X (PLC4Go) allow a malicious device, or an attacker able to inject network traffic, to crash or exhaust the memory of the client application, causing a denial of service. The individual defects are: - Generated parsers pre-allocate arrays with the element count claimed on the wire (0.13.0 through 0.13.1). - Transport read helpers		

CVE-2026-102510	allocate buffers of the size claimed on the wire without an upper bound. - ADS and KNXnet/IP response handling indexes into received data without checking its length, causing a panic. - ADS and EIP frame-length handling accepts, or arithmetically wraps to, a length of zero, breaking message framing. - Recursive protocol types are parsed without a nesting-depth limit. The same defect in the Java implementation is covered by CVE-2026-102509 https://cveprocess.apache.org/cve5/CVE-2026-102509 . Additionally, length and position arithmetic in generated serializers was performed in 16-bit integers. If an application forwards attacker-influenced payloads larger than 8 KB, the length field wraps, and the remainder of the payload may be interpreted by the receiving device (for example, an ADS PLC) as additional, independent protocol messages. This issue affects Apache PLC4X: from 0.11.0 before 1.0.0. PLC4Go is consumed as the Go module github.com/apache/plc4x/plc4go ; versions refer to the corresponding Apache PLC4X releases. Users are recommended to upgrade to version 1.0.0, which fixes the issue.	N/A	More Details
CVE-2026-104807	DigitalCanion has discovered a stored Cross-Site Scripting (XSS) vulnerability that allows an authenticated malicious user to inject persistent JavaScript or HTML content into the web application. The specific flaw exists within the web portal listening on TCP port 443, under Configuration → Domains, specifically in the “Description” field. The application fails to properly validate or sanitize user-supplied input before storing and subsequently rendering the field. By injecting malicious JavaScript into the Description field, an attacker can modify the content and behavior of the affected page when it is viewed by other users. This could allow an attacker to alter the page's appearance, display attacker-controlled content, or construct convincing phishing scenarios within the application's trusted web context.	N/A	More Details
CVE-2026-104808	DigitalCanion has discovered a stored Cross-Site Scripting (XSS) vulnerability that allows an authenticated malicious user to inject persistent JavaScript or HTML content, resulting in a denial-of-service condition within the web application. The specific flaw exists within the web portal listening on TCP port 443, under Configuration → Users → Users List. The vulnerability occurs in the “Microsoft Exchange mailbox” field, which fails to properly validate or sanitize user-supplied input before storing and rendering it. By injecting malicious JavaScript into this field, an attacker can cause the payload to execute whenever the affected user properties are accessed. This can prevent access to the affected user properties and result in a denial-of-service condition within the application's user-management functionality.	N/A	More Details
CVE-2026-102511	Improper Verification of Source of a Communication Channel in the ADS discovery of the Go implementation of Apache PLC4X (PLC4Go) allows an attacker able to send UDP datagrams to the discovering host to redirect subsequent connections to an arbitrary, attacker-chosen address. The discovery result's connection address was derived from the AmsNetId claimed in the response body rather than from the datagram's actual source address. One spoofed discovery response can therefore insert an inventory entry pointing at any host, including hosts outside the local network, and an application that connects to discovered devices will open its ADS session, including any configured route credentials, to that host. Additionally, discovery listeners in both implementations can be disabled by a single malformed datagram: - In PLC4Go ADS discovery, a short version block causes a panic that ends the listener for the rest of the discovery call, so legitimate devices answering afterwards are not reported. - In PLC4J, the ADS and EtherNet/IP discoverers stop on an unhandled exception from a malformed response. - The PLC4J Modbus discoverer can be made to spin indefinitely, consuming a CPU core, by a scanned host that sends a partial response. Exploitation requires the application to invoke the discovery API, which is opt-in, and for the connection redirect, to act on the discovered items. This issue affects Apache PLC4X: PLC4Go from 0.11.0 before 1.0.0; PLC4J ADS and Modbus drivers from 0.10.0 before 1.0.0; PLC4J EtherNet/IP driver from 0.11.0 before 1.0.0. PLC4Go is consumed as the Go module github.com/apache/plc4x/plc4go ; versions refer to the corresponding Apache PLC4X releases. Users are recommended to upgrade to version 1.0.0, which fixes the issue. Version 1.0.0 derives the connection address from the datagram's source address and logs a warning when the claimed AmsNetId disagrees with it.	N/A	More Details
CVE-2026-100103	Perforce P4 Search container images prior to 2026.4.2 reset the service authentication token to a publicly documented default value. An unauthenticated attacker with network access can obtain the highest application privilege, potentially leading to arbitrary code execution and compromise of the connected P4 Server.	N/A	More Details
CVE-2026-102778	Joomla Extension - svenbluege.de - Cross-site scripting and open redirect on the share mini page in Event Gallery extension < 6.6.0 - The page a shared image link opens (the share mini page of the front end) can link the article the image was shared from when the option "Share article links" is on. It took the address of the article from the shared link and printed it into the page without checking or escaping it; with the link type "Image Page with Redirect" it followed the address at once. A prepared link could therefore run a script in the page, in the session of the visitor who opened it, or send the visitor to another web site. Nothing on the server is changed or read by the server.	N/A	More Details
	Joomla Extension - svenbluege.de - Cross-site request forgery of list tasks of the backend in Event		

CVE-2026-102776	Gallery extension < 6.6.0 - Eight tasks which the buttons of the back-end lists call did not check the form token: setting the default payment method, shipping method, image type set, order status and watermark; putting an event into the shop or taking it out; choosing the main image of an event and whether an image is shown only as the main image; and sorting the images of an event. A prepared page on another web site could trigger them in the name of a logged in administrator and change those settings and flags. Nothing can be deleted or read this way; orders are not affected.	N/A	More Details
CVE-2026-93322	A malicious frontend can submit an LLB definition that causes buildkitd to panic and terminate, interrupting all builds running on that daemon.	N/A	More Details
CVE-2026-102984	Astro is a web framework for content-driven websites. Prior to 11.1.3, the @astrojs/node adapter builds a request URL from the Host header, and a malformed port can make that URL invalid. The recovery path reuses the same malformed host and throws an uncaught TypeError: Invalid URL before routing begins. In the default standalone configuration, the request returns an HTTP 500 response and the server continues running, but when staticHeaders is enabled the synchronous handler does not catch the exception and the Node process terminates. Proxies and CDNs that reject malformed Host headers prevent this path from reaching the origin. The issue affects availability only and does not expose data or permit code execution. This issue is fixed in version 11.1.3.	N/A	More Details
CVE-2026-104810	This vulnerability allows remote attackers to delete sensitive files on vulnerable installations of Mitel MiVoice Office 400. Authentication is required to exploit this vulnerability. The specific flaw exists within the web portal listening on TCP port 443, under Maintenance → File Management → File Browser, which is affected by a directory traversal vulnerability. By exploiting this vulnerability, an authenticated attacker can access and delete files outside of the intended directory, including files belonging to the Mitel application and the underlying Linux system. Deleting critical system or application files can result in a denial-of-service condition affecting the underlying system.	N/A	More Details
CVE-2026-104811	DigitalCanion SA has discovered a vulnerability that allows remote attackers to execute arbitrary code on affected installations of the product. Authentication may be required to exploit this vulnerability. The specific flaw exists within the Configuration → Services → Music on Hold functionality of the web portal listening on TCP port 443. The application is intended to allow users to upload WAV audio files but fails to properly validate the uploaded file type. An attacker can exploit this behavior to upload a malicious shared object (.so) instead of a WAV file. When the uploaded file is subsequently processed by the affected component, attacker-controlled code is loaded and executed in the context of the affected process. This can result in remote code execution and potentially full compromise of the underlying Linux system.	N/A	More Details
CVE-2026-102428	Joomla Extension - ordasoft.com - Unauthenticated SQL injection in OrdaSoft Joomla CCK < 8.3.16 - The order column for records was user provided and not properly validated, leading to a SQL injection vector.	N/A	More Details
CVE-2026-105689	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, app.util.ssr/blocked-address? relies on Java InetAddress predicates that do not classify NAT64, 6to4, or Teredo addresses and applies additional CIDR checks only to IPv4 values. Exploitation requires routing through a NAT64 gateway or an attacker-controlled DNS AAAA record; cloud environments with NAT64 gateways are directly exploitable. A user controlling a media import URL, or an administrator controlling a webhook URL, can then supply an IPv6 transition address that embeds a cloud-metadata, loopback, link-local, or private IPv4 target and bypasses the intended SSRF restrictions. Media import can disclose response bodies, while webhook delivery can expose response status as a network-probing side channel. This issue is fixed in version 2.18.0.	N/A	More Details
CVE-2026-105686	Penpot is an open-source design and prototyping platform. Prior to 2.18.0, the chunked media upload RPC validates that a chunk index is in range but neither rejects an already stored index nor replaces its previous object. An authenticated user can repeatedly upload the same valid index, causing each successful request to allocate another temporary object and increasing stored bytes beyond the upload session's declared logical size. Assembly detects the inconsistent chunk count only after allocation. This issue is fixed in version 2.18.0.	N/A	More Details
CVE-2026-102426	Joomla Extension - joomshaper.com - Reflected XSS in the Dynamic Content Filter addon in SP Page Builder Pro 3.0.0 - 5.6.1p2 - The slider minimum and maximum values are taken from the dc_filter_<fieldId> request parameter, split on the delimiter "I-r", HTML-escaped inside the data-value attribute, and then echoed without escaping as the span element's text content. An unauthenticated attacker reflects arbitrary HTML or JavaScript into the rendered page through a crafted dc_filter_<fieldId> value.	N/A	More Details
	Plane is an open-source project management tool. Prior to 1.4.0, Plane validates GITEA_HOST only for its URL scheme and does not reject hosts that resolve to private or internal IP addresses. The four		

CVE-2026-104976	outbound requests in the Gitea OAuth flow are derived from this unvalidated host and do not call validate_url(). In addition, avatar_url is taken from the Gitea user's profile, where users can configure external avatar URLs. After an administrator enables Gitea OAuth for a legitimate instance, a Gitea user can set an internal URL as the profile avatar and log in through Gitea, causing Plane to fetch the internal target without validation. This issue is fixed in 1.4.0.	N/A	More Details
CVE-2026-74865	sogo_yhn configures SOGo with a parameter "SOGoTrustProxyAuthentication=YES". This causes the password to be bypassed during HTTP Basic authentication. An unauthenticated attacker who provides the username of an existing user and any arbitrary password can successfully log in to that user's account. This issue was fixed in version 5.8.0~ynh9.	N/A	More Details
CVE-2026-74864	sogo_yhn configures SOGo with a parameter that forces the request with HTTP header "x-webobjects-remote-user" to be treated as sent by a verified user without performing password validation. Since Nginx does not strip this header, any client can supply it arbitrarily and gain access as any user, including a privileged user, without providing a password. This issue was fixed in version 5.8.0~ynh9.	N/A	More Details
CVE-2026-93903	LiteSpeed Web Server (LSWS) before 6.3.7 build 1 mishandles internal redirect URL validation in a certain "corner case."	N/A	More Details
CVE-2026-102983	Astro is a web framework for content-driven websites. From 5.2.0 until 8.2.4, the @astrojs/netlify adapter generates regular expressions for Netlify Image CDN remote-image allowlists without anchoring them to the beginning of the URL. Because Netlify evaluates these expressions with RegExp.test(), an allowed origin appearing only in a source URL's path or query can satisfy image.domains or image.remotePatterns while the URL's actual host remains attacker-controlled. An unauthenticated request to the public /.netlify/images endpoint can therefore cause the Image CDN to request attacker-selected URLs and may probe or reach internal services. Netlify egress protections may constrain reachable targets, and image transformation limits direct response exfiltration; no confidentiality or integrity impact has been demonstrated. This issue is fixed in version 8.2.4.	N/A	More Details
CVE-2026-103235	MISP contains a mass assignment vulnerability in the event delegation feature. When a user with delegation permission submits a delegation request, the application authorized the user against the event identified in the URL but then persisted the entire submitted record, including caller-supplied fields such as the primary key and event_id. An authenticated attacker could inject a primary key or event_id into the delegation payload to retarget an existing delegation record to any event on the instance. Because a delegation row grants the requesting organisation read access to the event it references, this effectively granted read access to arbitrary events belonging to other organisations. If the target organisation subsequently accepted the delegation, ownership of the event was transferred and the original record was deleted. Preconditions: - An authenticated user with the delegation permission (perm_delegate) - The MISP.delegation server setting must be enabled Impact: - Confidentiality: read access to any event on the instance - Integrity: overwriting existing delegation records and transferring event ownership Affected versions: MISP < 2.5.48	N/A	More Details
CVE-2026-103237	MISP contains an improper input validation vulnerability in its ORM save path. When a user submits data through various endpoints (attribute add/edit, event edit, free-text import, sighting capture, shadow attribute proposal, event report creation, object reference add, user admin edit), the application sanitizes the flat record by stripping the primary key and pinning the event_id or object_id to the caller's context. However, the underlying ORM's set() method gives priority to a nested key whose name matches the model alias and discards the outer scalar fields. An authenticated user with basic write permissions can exploit this by embedding a nested block under the model alias key inside their request. The sanitization logic (id removal, event_id pinning) is applied to the outer record, but the ORM binds to the inner record instead, which carries an attacker-chosen id and event_id. This allows the attacker to overwrite, re-parent, or soft-delete rows belonging to other organizations or events they have no read access to. Impact: - Cross-tenant data integrity compromise (attribute values rewritten, objects re-parented to attacker events, rows soft-deleted) - Affects multiple entity types: Attribute, Object, EventReport, Sighting, AttributeTag, ShadowAttribute - Requires only a low-privilege authenticated account with perm_add Affected versions: <2.5.48	N/A	More Details
CVE-2026-103239	MISP contains a privilege escalation vulnerability in the tag collection creation and editing functionality. The affected actions accepted the full HTTP request payload and passed it to a bulk-association save operation, which writes not only the intended tag collection record but also any associated model data present in the payload. A user holding the tag editor permission could craft a request that includes additional model data (such as User or Organisation records) alongside the tag collection fields. Because the save operation processed all associated models indiscriminately, the injected sibling records were written to the database, enabling the attacker to modify or create privileged accounts and escalate to site administrator. Preconditions: - An authenticated account with the tag editor permission (perm_tag_editor) - Network access to the MISP instance Impact: - Unauthorized creation or modification of User and Organisation records - Privilege escalation from tag editor to site administrator	N/A	More Details

	Affected versions: < 2.5.48		
CVE-2026-103602	Improper certificate validation in PkixNameConstraintValidator in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who controls, or can obtain certificates from, a name-constrained intermediate CA to have certificates accepted during PKIX certification path validation for email addresses, DNS names or URI hosts that lie within excluded subtrees applying to that CA, via an rfc822Name, dNSName or uniformResourceIdentifier name whose host ends with a dot, because names and constraints were compared without first removing the RFC 1034 root-label trailing dot, so a fully qualified host name did not match an excluded subtree for the same host written without the dot.	N/A	More Details
CVE-2026-100102	Perforce P4 Search container images prior to 2026.4.2 enable an unauthenticated Java debug interface. An attacker with network access to this interface can execute arbitrary code as the P4 Search service account, potentially leading to compromise of the connected P4 Server.	N/A	More Details
CVE-2026-55394	Unencrypted traffic in the 802.11 network of Teledyne FLIR Aware2 versions through 6.9.0.2 allows adjacent unauthenticated attackers to intercept, hijack, or modify session traffic against Teledyne FLIR PackBot robots running this software via sniffing or hijacking network traffic.	N/A	More Details
CVE-2026-86536	Improperly controlled modification of object prototype attributes ('prototype pollution') vulnerability in Apache Thrift all JS bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0 and re-generate JS code, which fixes the issue.	N/A	More Details
CVE-2026-86535	Loop with unreachable exit condition ('infinite loop'), Improperly controlled modification of object prototype attributes ('prototype pollution') vulnerability in Apache Thrift NodeJS bindings with TJSPONProtocol. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-85088	Improper Validation of Certificate with Host Mismatch in the C++ and D libraries of Apache Thrift. Both libraries install a default access manager for client sockets — TSSLConnectionFactory does so in C++, and the accessManager property does so in D — which compares the peer certificate against the host name that was connected to. That comparison walks the subjectAltName dNSName entries first and consults the certificate Common Name afterwards. A name that does not match yields a "skip" result rather than a rejection, so a certificate whose subjectAltName entries are all present and all non-matching falls through to the Common Name, which can then satisfy the check. RFC 6125 section 6.4.4, and RFC 9525 section 2, require that the Common Name is not consulted when a dNSName subjectAltName is present. A certificate carrying subjectAltName entries for one name and a Common Name for another is therefore accepted for a connection to the second name. Exploitation requires an attacker positioned on the network path who holds a certificate that chains to a certificate authority in the client's trust store and whose Common Name matches the connected host name. Public certificate authorities have not issued on Common Name alone for many years, so this is principally a concern for deployments using a private or enterprise public-key infrastructure. This issue affects the C++ library of Apache Thrift from 0.7.0 through 0.24.0 and the D library from 0.9.0 through 0.24.0. Users should upgrade to 0.25.0.	N/A	More Details
CVE-2026-85087	Improper certificate validation, Return of wrong status code vulnerability in Apache Thrift python bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-85086	Improper certificate validation, Initialization of a resource with an insecure default vulnerability in Apache Thrift perl bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-82459	Integer underflow (wrap or wraparound), Out-of-bounds write vulnerability in Apache Thrift C++ 32 bit THeaderTransport. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-82458	Memory allocation with excessive size value, Allocation of resources without limits or throttling vulnerability in Apache Thrift Go, netstd, OCaml, Erlang, JavaME, Rust, C++, Java, Kotlin and D language bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-61373	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Java TSaslNonblockingServer. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. In versions 3.3.22 and prior, an authenticated stored Cross-Site Scripting (XSS) vulnerability exists in the page backup viewer (admin/backup-edit.php). Page fields are correctly HTML-encoded when a page is saved, but the backup viewer decodes them again (htmldecode() / strip_decode()) and prints the result without re-escaping. A user who can edit a page can store	N/A	More Details

70650	JavaScript in a page's Keywords, Description, Menu text or Content; it executes in the browser of any administrator who later views that page's backup, in the context of the admin control panel. At time of publication, there are no publicly available patches.		
CVE-2026-71426	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. In versions 3.3.22 and prior, an authenticated user with page-editing rights can store an arbitrary filesystem path in a page's template attribute. On the public front-end, this value is passed unsanitized to a PHP include() when the page is rendered. Because the include path is never confined, this allows directory-traversal Local File Inclusion: arbitrary local files are included (and, if they contain PHP, executed) when any visitor requests the page. At time of publication, there are no publicly available patches.	N/A	More Details
CVE-2026-71542	GetSimple CMS is a content management system (CMS), and GetSimple CMS CE is the community edition of that CMS. In versions 3.3.22 and prior, GetSimpleCMS-CE is vulnerable to stored Cross-Site Scripting (XSS) in the "Theme to Components" functionality (admin/components.php) via the title parameter. The stored title is rendered inside a double-quoted HTML attribute in the administrative interface through an output path that HTML-entity-decodes the value before printing it, without re-encoding for the attribute context. This allows persistent execution of arbitrary JavaScript in the admin panel. At time of publication, there are no publicly available patches.	N/A	More Details
CVE-2026-102370	Kasa EC70 v4 and EC71 v4 do not logically disable the production debug interface at the firmware or chip level and do not lock the bootloader. Although the debug traces are physically severed during manufacturing, an attacker with physical access can restore the connection, interrupt the boot process, and manipulate boot parameters to enter a non-standard initialization path that exposes an unauthenticated root shell during startup. Successful exploitation may allow an attacker with physical access to obtain root-level command access during device startup, resulting in loss of confidentiality, integrity, and availability for the affected device. Exploitation requires device disassembly, restoration of the severed debug connection, and manipulation of the boot process.	N/A	More Details
CVE-2026-102514	Out-of-bounds Write (CWE-787) in the PEA archive extraction routine (pea.pas, unpea_procedure) of the first-party pea component in PeaZip 11.2.0 and earlier allows an attacker who convinces a victim to open or extract a crafted .pea archive to execute arbitrary code as the user running PeaZip. While decompressing a PCOMPRESS1 stream, the 32-bit compressed-block-size field of the first block (compsize) is read directly from the archive and used without validation as the length of a blockread into the fixed-size global buffers wbuf1/wbuf2 (1,114,112 bytes) and as the bound of the subsequent copy loop. The existing check "compsize > WBUF_SIZE" is applied only to the size of each following block, so the first block escapes it; the same unvalidated value is also used to index wbuf1[compsize], an out-of-bounds read at an attacker-chosen offset. The copy loop additionally copies the requested length instead of the number of bytes actually read, and terminates on equality rather than on an upper bound. Because the project is built without range checking and no archive password, integrity tag or non-default configuration is required, the overflow overwrites adjacent global data; code execution was demonstrated by two independent researchers against the official Linux x86-64 and Windows x64 builds, and the denial-of-service and memory-corruption primitive is cross-platform (Windows, macOS, Linux, BSD).	N/A	More Details
CVE-2026-55393	Unvalidated pathnames in the web interface in Teledyne FLIR Aware2 versions through 6.9.0.2 (PackBot) and 1.7.9 (FirstLook) allows remote unauthenticated attackers to read configuration and security parameters on Teledyne FLIR PackBot and FirstLook robots running this software via path traversal.	N/A	More Details
CVE-2026-55395	Hardcoded passwords in the access control in Teledyne FLIR Aware2 versions through 6.9.0.2 (PackBot) and 1.7.9 (FirstLook) allows remote unauthenticated attackers to access and reconfigure Teledyne FLIR PackBot and FirstLook robots running this software via reading the passwords from the firmware or documentation.	N/A	More Details
CVE-2026-100727	An improper access control vulnerability exists in GROWI, which allow an unauthenticated attacker to read files contained in non-public pages of the affected product when the file upload setting is configured as "Local".	N/A	More Details
CVE-2026-55396	Cleartext transmission without a cryptographic integrity check in operator control unit to robot UDP traffic in Teledyne FLIR Aware2 versions through 6.9.0.2 (PackBot) and 1.7.9 (FirstLook) allows adjacent unauthenticated attackers to intercept, hijack, or modify control traffic against Teledyne FLIR PackBot and FirstLook robots running this software via sniffing or hijacking network traffic.	N/A	More Details
CVE-2026-71451	- OS Command Injection vulnerability in Johnson Controls EasyIO FS32 allows - Command Injection. This issue affects EasyIO FS32: before 3.0b63.	N/A	More Details

CVE-2026-96780	figlet.js is a FIG driver written in JavaScript that aims to implement the FIGfont specification. Prior to 1.11.3, text() and textSync() can enter an unbounded loop when whitespaceBreak is enabled and width is smaller than the rendered width of a single FIGlet character. Under these conditions, breakWord() cannot find a valid break point and returns without consuming a character, so generateFigTextLines() repeatedly processes the same input while consuming CPU and growing memory. The non-default option and attacker-controlled width must both reach an affected call. This issue is fixed in version 1.11.3.	N/A	More Details
CVE-2026-18397	This vulnerability enables unauthenticated remote code execution (RCE) on a victim's machine by exploiting a combination of cryptographic weaknesses and memory management issues in the SConnect native host component. The attack leverages an unrestricted messaging interface between an attacker-controlled web page and the native host, allowing malicious input to bypass security checks.	N/A	More Details
CVE-2026-27873	- Use of Hard-coded Credentials vulnerability in Johnson Controls EasyIO FG allows - Pasword Spraying. This issue affects EasyIO FG: before 2.0b52.	N/A	More Details
CVE-2026-34493	- On-Chip Debug Interface vulnerability in Johnson Controls EasyIO FS32 allows Collect Data from Common Resource Locations. This issue affects EasyIO FS32: before 3.3b63.	N/A	More Details
CVE-2026-34494	- On-Chip Debug Interface vulnerability in Johnson Controls Neo Series MVP2 allows Collect Data from Common Resource Locations. This issue affects Neo Series MVP2: before 3.3b63.	N/A	More Details
CVE-2026-51882	The OpenAI-compatible file upload endpoint `/v1/files` in Langchain-Chatchat 0.3.0 is vulnerable to path traversal. An attacker can write files to arbitrary locations outside the `openai_files` directory by crafting malicious filenames.	N/A	More Details
CVE-2026-64892	- Exposure of Sensitive Information vulnerability in Johnson Controls Easy IO Neo allows Collect Data from Common Resource Locations. This issue affects Easy IO Neo: before 3.3b63.	N/A	More Details
CVE-2026-64893	- Cleartext Transmission of Sensitive Information vulnerability in Johnson Controls EasyIO NEO allows - Man In the Middle Attack. This issue affects EasyIO NEO: before 3.3b25.	N/A	More Details
CVE-2026-71448	: Insecure Default Initialization of Resource vulnerability in Johnson Controls EasyIO FS32 allows : Authentication Abuse. This issue affects EasyIO FS32: before 3.0b63.	N/A	More Details
CVE-2026-71449	: Use of Hard-coded Cryptographic Key vulnerability in Johnson Controls EasyIO FS32 allows : Retrieve Embedded Sensitive Data. This issue affects EasyIO FS32: before 3.0b63.	N/A	More Details
CVE-2026-71452	- OS Command Injection vulnerability in Johnson Controls EasyIO FS32 allows OS Command Injection. This issue affects EasyIO FS32: before 3.0b63.	N/A	More Details
CVE-2026-71453	- External Control of File Name or Path vulnerability in Johnson Controls EasyIO FS32 allows - traversal attack. This issue affects EasyIO FS32: before 3.0b63.	N/A	More Details
CVE-2026-86537	Uncaught exception, Loop with unreachable exit condition ('infinite loop'), Integer underflow (wrap or wraparound) vulnerability in Apache Thrift D language bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-87117	NULL pointer dereference vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-90440	Uncaught exception, improper handling of exceptional conditions, improper resource shutdown vulnerability in Apache Thrift D thrift.server.nonblocking.TNonblockingServer. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-92834	Use of uninitialized resource, Return of wrong status code vulnerability in Apache Thrift C++ WebSocket server. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details

CVE-2026-94655	Allocation of resources without limits or throttling, Inefficient Algorithmic Complexity vulnerability in Apache Thrift Lua bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94654	Loop with unreachable exit condition ('infinite loop') vulnerability in Apache Thrift python bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-85476	Loop with unreachable exit condition ('infinite loop') vulnerability in Apache Thrift c_glib bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-14983	Missing authentication in the web interface in Teledyne FLIR Aware2 versions through 6.9.0.2 allows remote unauthenticated attackers to achieve denial of service against Teledyne FLIR PackBot robots running this software via misuse of the reboot endpoint.	N/A	More Details
CVE-2026-83745	Memory allocation with excessive size value, Improper handling of length parameter inconsistency vulnerability in Apache Thrift nodejs and D lang bindings. Both bindings' WebSocket server transports read the payload length out of the frame header and allocate that many bytes immediately, without checking that the bytes have arrived. A single ~14-byte frame therefore commits as much memory as it cares to declare -- measured at 513 MiB against the Node.js server and 2 GiB against the D transport -- and in the Node.js case the connection is left open afterwards, so the frame can simply be sent again. This issue affects Apache Thrift before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-83663	Uncontrolled Recursion vulnerability in Apache Thrift go bindings. Both Go transports satisfy a read out of a buffered frame and, when that frame yields no payload bytes, read the next frame and call `Read` again instead of looping. A peer produces such a frame for 4 bytes in `TFramedTransport` (a declared size of zero) or 18 bytes in `THeaderTransport` (a header block that fills the frame), so nothing bounds the depth. The Go stack limit is reached as a `fatal error`, which `recover()` cannot catch, so the whole process dies. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-83632	Allocation of resources without limits or throttling, Integer overflow or wraparound, Heap-based buffer overflow vulnerability in Apache Thrift. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66859	NULL Pointer Dereference, Use of Uninitialized Variable vulnerability in Apache Thrift c_glib bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66858	The protocol skip routine in several Apache Thrift bindings did not apply the binding's recursion limit, so a message that nests unknown fields deeply enough can exhaust the stack. Affected: the Python C++ accelerator (the pure-Python protocols are not affected), the PHP library and its thrift_protocol extension, and the Perl, Lua, Smalltalk and OCaml libraries. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66837	Stack-based Buffer Overflow, Integer Overflow or Wraparound vulnerability in Apache Thrift php bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66331	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Delphi bindings buffered transport. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66081	Access of Uninitialized Pointer vulnerability in Apache Thrift c_glib bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66055	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift C++, Java, Go, netstd, Python and Delphi bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-66054	Allocation of Resources Without Limits or Throttling, Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in Apache Thrift C++ bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-63772	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift go bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details

CVE-2026-61374	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Java bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-104733	User Impersonation in ProcessOnes XMPP Server ejabberd <= 26.04 allows an attacker to impersonate arbitrary users via unvalidated authzid parameter in SASL-PLAIN mechanism.	N/A	More Details
CVE-2026-14984	Cleartext transmission in the primary control endpoints of Teledyne FLIR Aware2 versions through 6.9.0.2 allows remote unauthenticated attackers to intercept, hijack, or modify session traffic against Teledyne FLIR PackBot robots running this software via sniffing or hijacking network traffic.	N/A	More Details
CVE-2026-55252	OpenRun is an open-source, self-hosted GitOps platform for deploying web apps and internal tools to Docker or Kubernetes. Prior to version 0.17.7, the restrictions on redirect URLs in openrun can be bypassed by attackers, leading to open redirect attacks. This issue has been patched in version 0.17.7.	N/A	More Details
CVE-2026-96294	Uncaught exception, Improper Handling of Exceptional Conditions vulnerability in Apache Thrift NodeJS bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-96292	Inefficient regular expression complexity, Inefficient Algorithmic Complexity vulnerability in Apache Thrift Lua bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-96288	Uncontrolled Recursion, Allocation of resources without limits or throttling vulnerability in Apache Thrift Erlang bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94653	Inefficient Algorithmic Complexity vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94652	Missing release of memory after effective lifetime vulnerability in Apache Thrift c++ bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94648	Allocation of resources without limits or throttling vulnerability in Apache Thrift dart bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94646	Uncaught exception, Improper validation of specified quantity in input, Improperly controlled modification of object prototype attributes ('prototype pollution') vulnerability in Apache Thrift nodejs bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94638	Allocation of resources without limits or throttling vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94637	Improper handling of highly compressed data (data amplification) vulnerability in Apache Thrift Go bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94636	Improper handling of highly compressed data (data amplification), Function call with incorrectly specified arguments, Improper validation of specified quantity in input vulnerability in Apache Thrift py bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-71454	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in CWE-79 - Cross-site Scripting CAPEC-63 allows Cross-Site Scripting (XSS). This issue affects CAPEC-63: before 3.0b63.	N/A	More Details
CVE-2026-104480	Discord libdave before 1.2.0 did not reject an MLS Welcome message when the resulting group roster contained an unrecognized participant. An attacker in control of the DAVE signaling path (the voice gateway, or an equivalent position able to add, alter, or withhold signaling messages to a client) could cause affected clients to accept an unauthorized member into the end-to-end encrypted media session, compromising the confidentiality and integrity of audio and video.	N/A	More Details
CVE-2026-	Improper access control in ManagedProvisioning prior to SMR Sep-2026 Release 1 allows local attackers to install arbitrary applications.	N/A	More Details

21140			
CVE-2026-103885	Asymmetric Resource Consumption vulnerability in Apache Directory LDAP API. A LDAP server using the LDAP API (like Apache DS) may consume 100% of a CPU core indefinitely when processing some badly crafted Telephone Numbers. This issue affects Apache Directory LDAP API: from 2.1.0 before 2.1.9. Users are recommended to upgrade to version 2.1.9, which fixes the issue.	N/A	More Details
CVE-2026-16000	Missing cryptographic step in the DSTU 7624 CCM mode implementation (KCcmBlockCipher) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who can observe encrypted messages of known or chosen content to forge ciphertexts with valid authentication tags, via messages encrypted without associated data. The cause is that the G1 block, which binds the nonce, the message length and the parameter flags into the CBC-MAC, was processed only when associated data was present. Without associated data the tag was a CBC-MAC of the plaintext alone, independent of the nonce. Only applications that use KCcmBlockCipher directly and supply no associated data are affected.	N/A	More Details
CVE-2026-103877	Deserialization of Untrusted Data vulnerability in Apache Directory LDAP API. A rogue/compromised LDAP server (or pre-TLS MITM) can answer a client's loadSchema() subschema search with a schema object that contains a serialized Java class, allowing some potential RCE. This issue affects Apache Directory LDAP API: from 2.1.0 before 2.1.9. Users are recommended to upgrade to version 2.1.9, which fixes the issue.	N/A	More Details
CVE-2026-16001	Exposure of the message authentication key through the encryption keystream in the stream mode of lesEngine (an lesEngine constructed without a block cipher) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote attacker who has observed one encrypted message with known plaintext to forge shorter messages of their choosing that the recipient accepts as authentic, via a crafted ciphertext and MAC tag, because the MAC key was taken from the key derivation output directly after a keystream as long as the message, while the derivation input depends only on the static key pair and fixed parameters. The keystream revealed by that one message therefore contains the MAC key for every sufficiently shorter message.	N/A	More Details
CVE-2026-91784	cjbassi/gotop is vulnerable to local argument injection via process termination functionality. The process name is passed directly to pkill without sanitization. A local attacker can create a process with a crafted name beginning with -- (e.g. containing a target user's UID). When the user running gotop invokes the kill feature on that process, pkill interprets the crafted name as a command-line option, terminating all processes owned by the targeted user. Product is no longer actively supported and the vulnerabilities have not been fixed. Vulnerability was confirmed at version 3.0.0; other versions were not tested but may also be affected.	N/A	More Details
CVE-2026-63566	Memory allocation with excessive size value in the DTLS handshake reassembly (DtIsReliableHandshake, DtIsReassembler) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote unauthenticated DTLS peer to cause a denial of service through memory exhaustion via crafted handshake message fragments, because the reassembly buffer for each incoming handshake message was allocated at the 24-bit length declared in the fragment header, without the check against the peer's maximum handshake message size that TLS already applied. A fragment carrying no payload can force an allocation of almost 16 MB, for each of up to 16 pending messages per handshake, before the handshake is authenticated. DTLS servers and DTLS clients are both affected; TLS is not.	N/A	More Details
CVE-2026-59671	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim's browser. The endpoint "/es/datatables/getemployeeetypesdatatable" is affected.	N/A	More Details
CVE-2026-59670	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim's browser. The "nomListaValidacion" parameter is affected - endpoint "/es/validationslists/assignList/Employee/45659".	N/A	More Details
CVE-2026-59669	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim's browser. The "name" parameter is affected - endpoint "/es/attachmenttypes/update/203336"	N/A	More Details
CVE-2026-63567	Observable discrepancy in lesEngine.DecryptBlock in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote attacker who has captured an IES or ECIES ciphertext, and who can submit modified ciphertexts for decryption under the same key pair, to recover its plaintext via a CBC padding-oracle attack, because in block-cipher mode the engine decrypts the ciphertext and removes its padding before verifying the MAC. A padding failure is therefore reported with a different error message, and without the MAC computation, compared with a MAC failure. Only applications that construct lesEngine directly with a padded block cipher, such as AES in CBC mode with PKCS#7 padding, are affected; stream-mode IES is not.	N/A	More Details

CVE-2026-63568	Allocation of resources without limits or throttling in the CMP/CRMF password-based MAC verifier (PKMacBuilder) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote unauthenticated attacker to cause a denial of service through CPU exhaustion via a CMP message or CRMF certificate request whose PBMPParameter declares a very large iteration count, because PKMacBuilder enforced its iteration-count ceiling only when the caller had supplied an explicit maximum through the PKMacBuilder(IPKMacPrimitivesProvider, int) constructor. With any other constructor, ProtectedPkiMessage.Verify and CertificateRequestMessage.IsValidSigningKeyPop performed as many hash iterations as the sender requested, up to about 2^{31} , before the MAC could be checked.	N/A	More Details
CVE-2026-63569	Improper input validation in DHAgreement.CalculateAgreement (MTI/A0 two-pass Diffie-Hellman) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an on-path attacker to make the local party compute an agreed value the attacker already knows, defeating the key authentication MTI/A0 is meant to provide. It also allows a malicious peer to learn the local static private key modulo the small factors of p-1, and to recover it entirely in groups with many such factors. The attack uses a crafted out-of-range or small-order ephemeral value, and works because that value is raised to the static private key without the range and subgroup-membership checks applied to DH public keys. Only applications that call DHAgreement directly are affected.	N/A	More Details
CVE-2026-93029	There is a stored XSS vulnerability allowing arbitrary code execution in the WHM Manage SSL Hosts interface.	N/A	More Details
CVE-2026-93697	There is a stored XSS vulnerability allowing arbitrary code execution in the WHM Mass Modify Accounts interface.	N/A	More Details
CVE-2026-93698	Insufficient validation allows arbitrary commands to be executed via the Multilang adminbin.	N/A	More Details
CVE-2026-103600	Uncontrolled recursion in the ASN.1 parser (Asn1InputStream, Asn1StreamParser) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote unauthenticated attacker to cause a denial of service via a crafted ASN.1 encoding of deeply nested constructed elements (for example SEQUENCE inside SEQUENCE, in definite-length DER or indefinite-length BER form), because each nesting level is parsed by a further recursive call with no bound on depth. About 2,000 levels (8 KB of DER) are enough to exhaust a 1.5 MB thread stack, the .NET main-thread default on Windows, and raise a StackOverflowException, which .NET cannot catch and which terminates the whole process; on threads with larger stacks, parse time instead grows quadratically with depth (about 9 seconds of CPU for a 64 KB input). Any path that parses untrusted ASN.1 is exposed, including X.509 certificates and CRLs, CMS/PKCS#7, PKCS#8/PKCS#12, OCSP and TLS Certificate messages.	N/A	More Details
CVE-2026-63578	Allocation of resources without limits in password-based private-key decryption (PbeUtilities.GenerateCipherParameters) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who can supply an encrypted private key, such as a PKCS#8 EncryptedPrivateKeyInfo or "ENCRYPTED PRIVATE KEY" PEM file, to cause a denial of service through CPU exhaustion via an iteration count close to 2^{31} , because the count is taken from the unauthenticated algorithm parameters without an upper bound and the key derivation runs before the password or the data can be checked. PKCS#5 PBES1 and PBES2 (PBKDF2), the PKCS#12 PBE algorithms and CMS password recipients (CmsPbeKey) are affected. Loading PKCS#12 files with Pkcs12Store is covered by CVE-2026-63572, and a zero or negative count with the PKCS#12 algorithms by CVE-2026-63575.	N/A	More Details
CVE-2026-63577	Improper certificate validation in the directoryName name-constraint check (PkixNameConstraintValidator.WithinDNSubtree) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who controls, or can have certificates issued by, a name-constrained intermediate CA to get certificates accepted by PKIX path validation whose subject distinguished name, or a directoryName subjectAltName, lies outside the CA's permitted subtrees, via a name that places other RDNs ahead of a copy of the permitted RDN sequence, because the check looks for the constraint's first RDN anywhere in the name and compares the remaining RDNs from that position, instead of requiring the constraint to be an initial prefix of the name as RFC 5280 sections 4.2.1.10 and 7.1 require.	N/A	More Details
CVE-2026-63576	Improper certificate validation in PkixNameConstraintValidator (ExtractHostFromURL) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a name-constrained subordinate CA, or anyone able to obtain certificates with chosen subjectAltName URIs from such a CA, to bypass permitted or excluded uniformResourceIdentifier name constraints during certification path validation via a URI whose path, query, fragment or userinfo contains characters such as '@' or ':', because the host was extracted by string slicing without first isolating the RFC 3986 authority component, so the host compared against	N/A	More Details

	the constraints could differ from the URI's actual host.		
CVE-2026-63575	Loop with unreachable exit condition in the PKCS#12 key derivation (Pkcs12ParametersGenerator) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who can supply a PKCS#12 (PFX) file, or a PKCS#8 encrypted private key that uses a PKCS#12 password-based encryption algorithm, to cause a denial of service through CPU exhaustion via an iteration count of zero or below, because the derivation loop ran until its counter equalled the count, so for such a count it wrapped through about 2^{32} iterations before the MAC or the password could be checked. A 75-byte PFX file with a negative MacData iteration count kept Pkcs12Store.Load busy for many minutes.	N/A	More Details
CVE-2026-63574	Memory allocation with excessive size value in the OpenPGP signature and user attribute subpacket parsers (SignatureSubpacketsParser.ReadPacket, UserAttributeSubpacketsParser.ReadPacket) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote, unauthenticated attacker who can supply a crafted OpenPGP public key, certificate or signature to cause a denial of service (OutOfMemoryException or memory exhaustion in the parsing process) via a subpacket header using the five-octet length form, because the declared length was used to size the subpacket buffer with no upper bound and without being compared with the size of the enclosing subpacket area or packet, so a few bytes of input could demand an allocation of up to about 2 GB before any subpacket data was read.	N/A	More Details
CVE-2026-63573	Observable discrepancy in the CMS RSA PKCS#1 v1.5 key-transport unwrap (KeyTransRecipientInformation.UnwrapKey) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote attacker who holds a captured CMS EnvelopedData message, and who can submit many modified messages to an application that decrypts them with the recipient's RSA private key and reveals how decryption failed, to recover the captured message's content-encryption key and so its content, via a Bleichenbacher-style adaptive chosen-ciphertext attack, because a key-transport ciphertext with invalid PKCS#1 v1.5 padding is rejected during unwrap with a distinct "bad padding in message." CmsException instead of being replaced by a random key, so it can be told apart from a correctly padded ciphertext, which fails only later at content decryption.	N/A	More Details
CVE-2026-63572	Allocation of resources without limits in PKCS#12 keystore loading (Pkcs12Store.Load) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who can supply a PKCS#12 (PFX) file to cause a denial of service through CPU exhaustion via an iteration count close to 2^{31} in the file's MacData or in the PBE parameters of an encrypted SafeContents or shrouded key bag, because the counts are taken from the file without an upper bound and the key derivation runs before the MAC or the password can be checked. A zero or negative count is covered by CVE-2026-63575. Pkcs12Utilities.ConvertToDefiniteLength is also affected.	N/A	More Details
CVE-2026-63571	Improper verification of cryptographic signature in the attribute certificate path validator (PkixAttrCertPathValidator, also used by PkixAttrCertPathBuilder) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote attacker to have a forged X.509 attribute certificate accepted as valid, and so obtain whatever roles or privileges an application grants on the strength of its attributes, via an attribute certificate that names a trusted attribute authority as its issuer but was not signed by it, because the RFC 3281 validation steps check the holder and issuer certification paths, validity period, extensions and revocation status but never verify the attribute certificate's signature with the issuer's public key. Only applications that use these classes to validate attribute certificates are affected.	N/A	More Details
CVE-2026-63570	Loop with unreachable exit condition in Pkcs12Store.GetCertificateChain in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an attacker who can supply a crafted PKCS#12 file to an application that loads it and requests a key entry's certificate chain to cause a denial of service, in which the call never returns and consumes CPU and memory until an OutOfMemoryException, via certificates whose issuer links form a cycle, for example two certificates whose AuthorityKeyIdIdentifier extensions each identify the other's public key. This happens because the chain-building loop stops only when no issuer is found or a certificate links to itself, and keeps no record of certificates already visited. The key-identifier links are followed without checking signatures.	N/A	More Details
CVE-2026-18036	In Bouncy Castle for Java before 1.86, NTRU reduced secret values with the % operator in three helpers whose reference implementations are deliberately division-free, so each reduction was carried out by an integer division whose latency depends on the secret operand. Polynomial.modQ divided by a variable divisor, which a compiler cannot strength-reduce to a multiply the way it can a constant one, so it emitted a division on every call including on the decapsulation path where the dividend derives from the private key; Polynomial.mod3 and NTRUSampling.mod3 divided the secret key polynomials f and g during key generation, the message polynomials r and m during encapsulation, and coefficients recovered during decapsulation. An attacker able to measure that timing can recover information about the NTRU private key. modQ now masks, which is exact because q is always a power of two, and mod3 uses the reference implementation's division-free fold and select; the results are unchanged.	N/A	More Details
	In Bouncy Castle for Java before 1.86, several password-based key derivation entry points ran the KDF		

CVE-2026-17508	with cost parameters taken from the untrusted input being processed, without bounding them, so a small input could dictate an arbitrary amount of work before any password or integrity check could reject it. The affected paths are the RFC 9579 PBMAC1 MAC calculator builders, which took the PBKDF2 iteration count and derived-key length straight out of PBMAC1Params (JcePbMac1CalculatorBuilder, and PKCS12PBEUtils.createPbMac1Calculator reached from PKCS12PfxPdu.isMacValid); the script parallelization parameter p in the PKCS#8 and PKCS#12 cost guards, which bounded only the cost parameter N and the block size r even though the scratch buffer scales with r times p, so the configured memory ceiling could be evaded entirely; the raw JCA PBKDF2 provider (org.bouncycastle.jcajce.provider.symmetric.PBEPBKDF2); and the bcrypt round count read from an encrypted OpenSSH v1 private key's own kdfoptions. Each now bounds the parameter before deriving, in line with the caps already applied elsewhere in the tree, with the OpenSSH round count configurable through the new org.bouncycastle.openssh.max_rounds property. This completes the bounding begun in 1.85 for the PKCS#8 / PBES2 decryptors (CVE-2026-15055). This issue also affects Bouncy Castle for Java LTS before 2.73.13, and Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).	N/A	More Details
CVE-2026-17507	In Bouncy Castle for Java before 1.86, the MLS implementation (org.bouncycastle.mls) holds RFC 9420's uint32 leaf_index in a signed int, so a wire value with the top bit set decodes to a negative number. That is a legitimate encoding rather than malformed input, and it must still decode, since the MLS interop test vectors round-trip the full range. GroupKeySet.SecretTree.hasLeaf and Group.validateRemove compared the decoded value directly against the tree's leaf count, and a signed comparison treats any negative int as less than a positive bound, so an out-of-range sender passed the membership check. In the hasLeaf case the SenderData of an unprotected PrivateMessage could then drive LeafIndex.directPath through NodeIndex.parent() arithmetic that never reaches the tree root, growing the resulting node list without bound until the JVM exhausted its heap. A single small message from any current group member could therefore deny service to every other member of the group. Both comparisons now interpret the value as unsigned via Integer.toUnsignedLong, rejecting an out-of-range sender however it was encoded; well-formed leaf indices are unaffected.	N/A	More Details
CVE-2026-103601	Release of unverified plaintext in the CCM (CcmBlockCipher) and DSTU 7624 CCM (KCcmBlockCipher) AEAD modes in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote attacker to obtain decryptions of ciphertexts of their choosing via forged messages sent to an application that lets the output buffer of a failed decryption be observed, for example through buffer reuse or logging, because decryption wrote the recovered plaintext into the caller-supplied output buffer before checking the authentication tag and left it there when the check failed. Only decryption into a caller-supplied buffer is affected; methods that return a newly allocated array are not.	N/A	More Details
CVE-2026-103604	Inefficient algorithmic complexity in X.509 distinguished name string conversion (X509Name.ToString and letfUtilities.ValueToString) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote unauthenticated attacker to cause a denial of service through CPU exhaustion via a certificate, CRL, certification request or other structure whose name contains a long attribute value made up of characters that must be escaped, such as commas, or of leading or trailing spaces, because each escaping backslash was inserted into the buffer being scanned, so the work grew quadratically with the length of the value. Applications are exposed when they convert such a name to a string, for example to log or display it, or compare it with letfUtilities.RdnAreEqual, as PKIX path validation does for directoryName name constraints.	N/A	More Details
CVE-2026-15999	Improper validation of integrity check value in the AES-CCM implementation (CcmParameters and CcmBlockCipher) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows an on-path attacker to modify CCM-encrypted content without detection via an AlgorithmIdentifier whose CCMPParameters declare an authentication tag (aes-ICVlen) of zero or another length outside the RFC 5084 set, because CcmParameters accepted any value and CcmBlockCipher validated the tag length only when encrypting, so decryption compared a zero-length or very short tag. Affected paths include ParameterUtilities.GetCipherParameters, used by CmsEnvelopedData and CmsEnvelopedDataParser for EnvelopedData encrypted with AES-CCM, and any caller passing an unchecked tag length to CcmBlockCipher for decryption.	N/A	More Details
CVE-2026-59659	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim's browser. The "nomZonaGeo" parameter is affected – endpoint "/es/geozones/update/149979".	N/A	More Details
CVE-2026-96990	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Erlang bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-59660	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim's browser. The "nomTransportista" parameter is affected – endpoint "/es/carriers/update".	N/A	More Details

CVE-2026-94651	improper handling of exceptional conditions, Missing release of resource after effective lifetime vulnerability in Apache Thrift java bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94650	Uncontrolled Recursion vulnerability in Apache Thrift c_glib bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94645	Improper validation of specified quantity in input, Allocation of resources without limits or throttling vulnerability in Apache Thrift nodejs bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94644	Allocation of resources without limits or throttling vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94642	Uncaught exception vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94633	Memory allocation with excessive size value, Improper handling of length parameter inconsistency vulnerability in Apache Thrift Dart bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-93926	Missing release of memory after effective lifetime, Missing release of resource after effective lifetime vulnerability in Apache Thrift THeaderTransport. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-93925	Stack-based buffer overflow, Incorrect bitwise shift of integer vulnerability in Apache Thrift C++ THeaderProtocol. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-91137	Improper validation of specified quantity in input, Allocation of resources without limits or throttling, Excessive Iteration vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-91135	Heap-based buffer overflow vulnerability in Apache Thrift C++ THeaderTransport. When an application enables the ZLIB transform for the frames it sends, THeaderTransport::transform() copies the compressed frame into the write buffer without making sure it fits. Data that does not compress, such as content a remote peer supplied, grows under compression, so the copy writes past the end of the heap buffer by an amount that grows with the size of the frame, and for large frames it also reads past the end of the transform buffer. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-86326	An improper verification of cryptographic signature vulnerability exists in protocol gateways because the device does not properly verify the cryptographic authenticity of firmware images before installation. An attacker with high privileges and access to the firmware update interface could provide a specially crafted or modified firmware image, causing it to be installed on the device. Successful exploitation could allow the attacker to execute unauthorized code, compromise the integrity and availability of the device, and persist malicious modifications across subsequent firmware updates.	N/A	More Details
CVE-2026-86325	A stack-based buffer overflow vulnerability exists in protocol gateways' account management interface. The vulnerability is caused by insufficient length validation of the `account_name` parameter when processing account management requests. An attacker authenticated as a read-only user to the web management interface could supply a specially crafted account name that exceeds the size of the internal stack buffer, resulting in corruption of program execution flow. Successful exploitation could allow an attacker to read sensitive information from device memory, including credentials, modify arbitrary memory contents, and disrupt device availability.	N/A	More Details
CVE-2026-85494	Improper handling of length parameter inconsistency, Uncaught exception, Inefficient Algorithmic Complexity, Memory allocation with excessive size value, Initialization of a resource with an insecure default vulnerability in Apache Thrift Python, Ruby, Erlang, Lua, Dart, JavaME, Perl, PHP and D language bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-85493	Uncontrolled Recursion vulnerability in Apache Thrift Dart and Java ME bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-	Use of uninitialized resource, Return of wrong status code vulnerability in Apache Thrift c_glib bindings.		More

2026-85483	This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	Details
CVE-2026-59668	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomTamano” parameter is affected – endpoint “/es/companysizebills/store”.	N/A	More Details
CVE-2026-59667	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomTamano” parameter is affected – endpoint “/es/companysizeemployees/update”.	N/A	More Details
CVE-2026-59666	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomOrigen” parameter is affected – endpoint “/es/origins/store”.	N/A	More Details
CVE-2026-95662	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomCompetidor” parameter is affected – endpoint “/es/competitors/store”.	N/A	More Details
CVE-2026-94639	improper handling of exceptional conditions, Allocation of resources without limits or throttling, Uncaught exception vulnerability in Apache Thrift Java bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94635	Allocation of resources without limits or throttling, Improper handling of length parameter inconsistency vulnerability in Apache Thrift Lua bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94634	Allocation of resources without limits or throttling, Initialization of a resource with an insecure default vulnerability in Apache Thrift Python bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-59673	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomTipoCli” parameter is affected – endpoint “/es/clienttypes/update/109441”.	N/A	More Details
CVE-2026-59672	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomGrupoEmpresarial” parameter is affected – endpoint “/es/corporategroups/update/246”.	N/A	More Details
CVE-2026-59665	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomMotivo” parameter is affected – endpoint “/es/lostmotives/store”.	N/A	More Details
CVE-2026-59664	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomServicioPrestado” parameter is affected – endpoint “/es/providedservices/store”.	N/A	More Details
CVE-2026-59663	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomDelegacion” parameter is affected – endpoint “/es/delegations/store”.	N/A	More Details
CVE-2026-59662	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomCompetidor” parameter is affected – endpoint “/es/competitors/store”.	N/A	More Details
CVE-2026-59661	Cross-Site Scripting vulnerability in the Repasat application. Successful exploitation of this vulnerability could allow an attacker to trick a user into executing arbitrary code in the victim’s browser. The “nomRuta” parameter is affected – endpoint “/es/routes/update/693”.	N/A	More Details
CVE-2026-94656	Allocation of resources without limits or throttling vulnerability in Apache Thrift ruby bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94657	Allocation of resources without limits or throttling vulnerability in Apache Thrift JavaME bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-94658	Inefficient Algorithmic Complexity vulnerability in Apache Thrift Lua bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details

CVE-2026-93495	Improper initialization in an ASUS certain motherboard allows an physically proximate user to read or write arbitrary memory by inserting a specially crafted device. Refer to the ' Security Update for Multiple ASUS Motherboards ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-76143	A missing authorization vulnerability in Genian SSL PNS allows an attacker to bypass multi-factor authentication by manipulating a login request parameter.	N/A	More Details
CVE-2026-76144	An unrestricted file upload vulnerability caused by insufficient file extension and integrity verification in Genian SSL PNS allows an attacker to upload a dangerous file that is not an official patch	N/A	More Details
CVE-2026-76145	An improper privilege management vulnerability in Genian SSL PNS allows an attacker to escalate to super administrator privileges and force the creation of an OS account by manipulating the permission column during CSV bulk user registration	N/A	More Details
CVE-2026-76146	An OS command injection vulnerability in Genian SSL PNS allows an attacker who knows only the client access ID, without the password, to execute arbitrary commands remotely	N/A	More Details
CVE-2026-76147	A path traversal (ZIP Slip) vulnerability caused by insufficient authorization and integrity verification in the agent upgrade feature of Genian NAC/ZTNA allows a remote attacker to execute arbitrary code	N/A	More Details
CVE-2026-78210	In affected versions of Octopus Server, users with certain scoped permission sets could execute arbitrary scripts in an environment without possessing the required authorization.	N/A	More Details
CVE-2026-103603	Memory allocation with excessive size value in the HSS/LMS signature code (HssPublicKeyParameters, HssSignature) in Legion of the Bouncy Castle Inc. bc-csharp before 2.7.0 allows a remote unauthenticated attacker who can supply both an HSS public key and a signature to cause a denial of service through memory exhaustion via a public key encoding with an excessive level count, because the level count L read when parsing an HSS public key was not checked against the RFC 8554 maximum of 8, and signature parsing then allocated an array of L - 1 entries before reading any further signature data. A single verification can commit up to about 17 GB of memory or fail with an OutOfMemoryException.	N/A	More Details
CVE-2026-103651	MISP contains a vulnerability in its one-time password (OTP) authentication flow that allows replay of a consumed HOTP (paper) token and rewinding of the token counter. The HOTP verification logic compared the submitted token against a counter value that was cached in the user's session at the time the password was entered, rather than against the authoritative counter stored in the database. Because the session-cached counter is not updated after a token is successfully consumed, an attacker who holds a valid session (password already submitted) can reuse a previously burned HOTP token. The stale cached counter still matches the replayed token, granting a second successful authentication and effectively rewinding the counter state. Preconditions: - The target user has HOTP (paper token) second-factor authentication enabled. - The attacker possesses a valid session in which the password step has already been completed (the OTP step is pending). - The attacker has access to at least one HOTP token value (e.g., a paper token list). Security impact: - Bypass of the second authentication factor, allowing unauthorized access to a user's MISP account. - Corruption of the HOTP counter state, potentially invalidating subsequent legitimate tokens or enabling further replays. Affected versions: <2.5.48.	N/A	More Details
CVE-2026-78249	A path traversal vulnerability exists in the web management interface of multiple Multifunction Devices and Printers, including Apeos C4571 1.1.3 and earlier, Apeos C3567 1.1.3, or other products listed, specifically in the handling of externally supplied parameters. If the device receives a specially crafted, malicious request, it may trigger unintended processing.	N/A	More Details
CVE-2026-103655	MISP contains a vulnerability in its two-factor authentication (TOTP) verification process that permits a valid one-time code to be accepted more than once within its time-based validity window. The issue exists in the user login flow where a TOTP code is verified as a second authentication factor. Because the system did not record whether a given TOTP period had already been consumed, the same code remained valid for its entire time window (typically 30 seconds). An attacker who captures a legitimate code during a user's login could replay it to authenticate a second session as that user. Preconditions: - The target user has TOTP-based two-factor authentication enabled. - The attacker is in a position to observe or intercept the TOTP code during a legitimate login (e.g., network-level interception, shoulder surfing, or a compromised client). - The replay must occur within the TOTP validity period. Security impact: - Unauthorized account access by replaying a captured one-time code. - Potential compromise of threat-intelligence data and administrative functions accessible to the targeted user. Affected versions: <v2.5.48.	N/A	More Details

CVE-2026-97873	In Bouncy Castle for Java before 1.86, the raw JCA provider's legacy PBES1 (PKCS#5 scheme 1) and PKCS#12 PBE families ran their password-based key derivation with an iteration count taken from untrusted input without bounding it, so a small input could dictate an arbitrary amount of work before anything could be verified. The AlgorithmParameters implementations (PKCS12PBE and its object identifier aliases, and PBKDF1) accepted any count from an encoded PKCS12PBEPParams or PBEParameter, narrowing a value beyond the int range with intValue(), and every Cipher, Mac and SecretKeyFactory in these families derived with whatever count it was given, including one decoded by another provider's AlgorithmParameters, as when javax.crypto.EncryptedPrivateKeyInfo.getKeySpec() decrypts a PKCS#12 PBE-protected private key with BC. Both the parameter parse and the derivations now reject a negative or over-limit count under the org.bouncycastle.pbe.max_iteration_count property (default 10,000,000) that already bounded PBKDF2 (CVE-2026-17508), and the parse rejects a count beyond the int range rather than narrowing it. This issue also affects Bouncy Castle for Java LTS before 2.73.13.	N/A	More Details
CVE-2026-85515	In Bouncy Castle for Java before 1.86, a truncated OpenPGP encrypted message was accepted with no error reported, and on the SEIPD version 1 path with no integrity check performed at all. RFC 9580 sec. 13.7 permits an implementation to release the cleartext of the fully authenticated chunks when streaming but requires it to indicate a clear error as soon as the truncation is detected, and to report suspect integrity when it discovers malleable ciphertext. The truncation was detected and then discarded: when a message is truncated but the length field of the enclosing packet is left unchanged, BCPGInputStream.PartialInputStream raises an EOFException for the missing ciphertext, and BCPGInputStream.nextPacketTag() reports an EOFException as a clean end of message, so the packet stream above it stopped as though no packets remained. On the AEAD path (SEIPD version 2 and the version 5 AEAD packet), when the literal data packet ended on an AEAD chunk boundary and the consumer read in increments smaller than one chunk, the look-ahead for the packet after the literal triggered the truncated chunk read, so BcAEADUtil and JceAEADUtil never reached the trailing message tag of sec. 5.13.2 that authenticates the total plaintext length; the caller received the plaintext of the fully authenticated chunks, every packet following the literal was silently dropped, and no exception was raised, so a signed and encrypted message read back as a well-formed unsigned one. Every byte released on that path remained individually authenticated, making this a missing truncation error rather than a forgery, and it is a residual of CVE-2026-12817, which closed the same outcome for an attacker who corrects the outer packet length. On the SEIPD version 1 path the consequence was more serious: IntegrityProtectedInputStream verifies the modification detection code from close(), and reached close() only by closing itself when a read of it returned -1, which a truncated message never produces, so PGPEncryptedData.verify() never ran and the recipient was handed CFB-decrypted plaintext on which no integrity check of any kind had been performed. Measured on a message truncated into that shape, 136 distinct single-byte modifications of the ciphertext produced accepted, altered plaintext with no exception raised. Reachability is a property of the message rather than of attacker-supplied input: the AEAD shape held for 3 of 131 consecutive payload lengths measured, and the SEIPD version 1 shape for one payload length in sixteen, at a truncation offset that did not move with the payload length. The low-level API is unaffected, a caller that invokes PGPEncryptedData.verify() directly getting the check regardless, as are consumers reading in increments of a whole AEAD chunk or more. The AEAD decryption streams now re-throw such an EOFException as a plain IOException, which nextPacketTag() does not launder; OpenPGPMessageInputStream.close() now closes its layer's integrity-protected stream itself rather than relying on that stream having seen the end of its data; and IntegrityProtectedInputStream.close() was made idempotent, as java.io.Closeable requires, which that depends on, since the stream is genuinely closed twice on the ordinary path and PGPEncryptedData.verify() consumes the digest state behind it and cannot be run a second time. This issue also affects Bouncy Castle for Java LTS before 2.73.13, on the AEAD route only, as that edition does not ship the high-level OpenPGP API the SEIPDv1 route runs through. It also affects Bouncy Castle for Java FIPS (BC-FJA) before bcpg-fips 1.0.14 (1.0.X series), 2.0.14.1 (2.0.X series) and 2.1.14 (2.1.X series), on the AEAD route only, as those editions do not ship the high-level OpenPGP API.	N/A	More Details
CVE-2026-71892	In Bouncy Castle for Java before 1.86, the opt-in key-size validation on CMS key-transport recipients, org.bouncycastle.cms.jcajce.JceKeyTransRecipient.setKeySizeValidation(true), never ran for a message using RFC 9709 content-encryption key derivation (id-alg-cek-hkdf-sha256). The branch that should have selected the actual content-encryption algorithm carried in the key derivation AlgorithmIdentifier's parameters compared the encrypted-key byte array against the id-alg-cek-hkdf-sha256 object identifier, a comparison between a byte array and an ASN1ObjectIdentifier that is false for every possible input, so the check fell through to a key-size lookup on the outer wrapper OID. That OID identifies a key-derivation construction rather than a cipher and has no registered key size, so the size comparison was skipped entirely. A key-transport EnvelopedData or AuthEnvelopedData whose transported, HKDF-derived content-encryption key did not match the key size of the advertised content-encryption algorithm was therefore accepted even with validation explicitly enabled, silently defeating the only mechanism the API offers for enforcing recovered key size. The recipient now dispatches on the content-encryption AlgorithmIdentifier's algorithm OID, so validation checks the recovered key	N/A	More Details

	against the inner content-encryption algorithm. Messages with a matching key size, non-HKDF messages, and recipients that do not enable validation are unaffected. This issue also affects Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).		
CVE-2026-71891	In Bouncy Castle for Java before 1.86, BLS12_381BasicScheme.keyValidate, and so BLSPublicKeyParameters and every BasicScheme, MessageAugmentation and ProofOfPossession verify and aggregateVerify that gate on it, accepted a public key built on a foreign ECCurve that merely shares BLS12-381's field characteristic. The prime-order subgroup check trusts a point's own curve to name its cofactor, since ECPPoint.satisfiesOrder returns true outright when the curve's cofactor is one, so a point on a curve with a different equation and a cofactor forged to one passed keyValidate despite not being a G1 point at all. In BC's pairing implementation such a point contributes the identity in the target group, so an aggregate signature verified against a set of public keys including it is accepted even though it contains no signature for that key and message pair, admitting a phantom signer. keyValidate now first confirms that the point's curve carries exactly the canonical G1 field, equation, order and cofactor before any subgroup check. The issue is reachable only where an application constructs an ECPPoint on an explicit, non-canonical curve and accepts it as an authority-bearing key; the standard 48-byte compressed-point decoder always supplies the canonical curve and was never affected.	N/A	More Details
CVE-2026-71890	In Bouncy Castle for Java before 1.86, validation of an MLS (RFC 9420) external commit's proposal list, org.bouncycastle.mls.protocol.Group.validateExternalCachedProposals, counted the proposals by type and bounded the removed leaf index but never established that the removed leaf had anything to do with the joiner. RFC 9420 sec. 12.2 permits at most one Remove proposal in an external commit, with which the joiner removes an old version of themselves, and requires that where one is present the LeafNode in the commit's path field meet the criteria it would have to meet in an Update for the removed leaf, in particular that its credential present identifiers acceptable for the removed participant. The ordinary proposal-list validator's self-remove rule is deliberately not applied on this path, because a resync commit legitimately removes a leaf the joiner owns, but nothing was put in its place. Any party holding the group's public GroupInfo, which is precisely what an external joiner is meant to be given, could therefore commit a Remove naming any member's LeafIndex and have every member apply it, evicting that member and taking over their slot in the ratchet tree. The credential check that should have prevented this existed only in the gRPC interop harness and so protected no other caller of the public Group.externalJoin and Group.handle API. An external commit carrying a Remove is now accepted only when the removed leaf's credential is identical to the one in the joiner's own new leaf, on both the sending and the receiving side.	N/A	More Details
CVE-2026-71889	In Bouncy Castle for Java before 1.86, neither copy of PKIXCertPathReviewer - org.bouncycastle.pkix.jcajce.PKIXCertPathReviewer nor the legacy org.bouncycastle.x509.PKIXCertPathReviewer - applied X.509 name constraints to the end-entity certificate. checkNameConstraints walked the path with a loop bound of index greater than zero, which is the bound the CA-only steps require, but index zero is the target certificate under the standard CertPath ordering, so the permitted and excluded subtree checks of RFC 5280 sec. 6.1.3 (b) and (c) never ran against the leaf's subject DN or its subjectAltName. A chain whose leaf violated a NameConstraints extension imposed by its own issuing CA therefore reported isValidCertPath() true with an empty error list, while CertPathValidator.getInstance("PKIX", "BC"), which shares no code with the reviewer, rejected the identical chain against the identical trust anchor. An application using the reviewer to make the trust decision rather than for diagnostics alongside a real validation accepted a certificate the constrained CA was never authorised to issue. Both copies now check every certificate in the path including the target, waive the sec. 4.2.1.10 self-issued exemption for the final certificate as sec. 6.1.3 requires, and skip the sec. 6.1.4 (g) constraint-accumulation step for the target. This issue also affects Bouncy Castle for Java LTS before 2.73.13, which carries only the org.bouncycastle.pkix.jcajce copy of the reviewer. It also affects Bouncy Castle for Java FIPS (BC-FJA) before bcpkix-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series).	N/A	More Details
CVE-2026-71888	In Bouncy Castle for Java before 1.86, the streaming CMS AuthenticatedData parser accepted a message whose digestAlgorithm and authAttrs fields disagreed about whether authenticated attributes were present. RFC 5652 sec. 9.1 pairs the two, requiring that authAttrs be present whenever digestAlgorithm is, and sec. 9.2 makes the MAC cover the DER encoding of authAttrs when they are present and the eContent OCTET STRING directly when they are not. CMSAuthenticatedDataParser has to choose between those two in its constructor, before it can reach authAttrs, which comes later in the SEQUENCE, so it chose on digestAlgorithm alone: for a message with digestAlgorithm absent but authAttrs present it verified the content MAC and then returned the attributes through getAuthAttrs() as though they had been authenticated, when the MAC had never covered them. An attacker able to modify a message in transit could insert an authenticated attribute, such as an RFC 2634 ESSSecurityLabel, into an otherwise valid message while holding neither the key-encryption key nor the content-MAC key, and an application taking an authorization, routing or labelling decision from those attributes would act on attacker-chosen values. The content itself remained MAC-bound. asn1.cms.AuthenticatedData now rejects the mismatched pairing when parsing and	N/A	More Details

	CMSAuthenticatedDataParser cross-checks the two fields once authAttrs is read. This is a variant of CVE-2026-59642, which bound the content to the MAC for messages that legitimately carry authAttrs, and which does not address this case. This issue also affects Bouncy Castle for Java LTS before 2.73.13, and Bouncy Castle for Java FIPS (BC-FJA) before bcpx-fips 1.0.13 (1.0.X series), 2.0.13 (2.0.X series) and 2.1.13 (2.1.X series), and bcutil-fips 2.0.8 (2.0.X series) and 2.1.8 (2.1.X series).		
CVE-2026-71887	In Bouncy Castle for Java before 1.86, the high-level OpenPGP API accepted a data signature made by a signing subkey whose Subkey Binding signature carried no embedded Primary Key Binding (cross-certification) signature, in the case where that binding omits a Key Flags subpacket. RFC 9580 sec. 5.2.1.8 and sec. 10.1.3 require the embedded Primary Key Binding signature on any subkey that can issue signatures; it is the subkey's own statement that it belongs to the primary key it is bound under. OpenPGPCertificate resolved the subkey's key flags two different ways. isSigningKey() goes through getKeyFlags() and getApplyingSubpacket(), which falls back to the primary key's direct-key or primary User ID self-signature when the binding signature omits the subpacket, so the subkey inherited the primary's SIGN_DATA and counted as signing-capable; verifyEmbeddedPrimaryKeyBinding(), which enforces the requirement, reads the binding signature's own hashed subpackets, found no SIGN_DATA there, and returned early as a non-signing key without ever demanding the back signature. The same subkey was therefore signing-capable - so its signatures were attributed to the certificate and OpenPGPSignature.OpenPGPDocumentSignature.isValid() returned true - while being exempt from cross-certification, where GnuPG refuses the identical certificate and message. An attacker needs only the victim's public signing subkey, which is public material: they bind it to their own primary key with a Subkey Binding signature they are able to make, carrying no Key Flags and no embedded Primary Key Binding signature, which they cannot make without the subkey's private key, and a relying party verifying one of the victim's genuinely signed messages against that certificate is told the signature is valid and given the attacker's certificate as its issuer. Because a certificate's User IDs are self-asserted, a verifier that pins on the subkey's fingerprint or key ID while taking the identity from the enclosing certificate reports a real signature under an attacker-chosen identity. This is misattribution of a genuine signature rather than forgery of a new one: no private key is recovered, and the signature must be one the grafted subkey actually made. The low-level PGPSignature / PGPPublicKeyRing API performs no binding checks by design and is unaffected. Key Flags are a statement about the key the carrying signature refers to (RFC 9580 sec. 5.2.3.29), so a subkey no longer inherits them from the certificate-wide signatures of the primary key: a Subkey Binding signature that omits the subpacket now leaves the subkey with no capabilities rather than the primary's, which makes the flags the cross-certification check consults the same flags every other decision consults. Preferences and the other subpackets a direct-key signature carries are inherited as before, and the primary key itself, whose flags legitimately come from its own direct-key or User ID self-signature, is unaffected.	N/A	More Details
CVE-2026-71886	In Bouncy Castle for Java before 1.86, the high-level OpenPGP certificate API accepted a third-party certification or trust delegation from any component key of the issuing certificate, without requiring that component to have been granted the authority to certify. OpenPGPCertificate.getCertificationBy() and getDelegationBy() resolve a third-party signature by matching its issuer key identifier against every key of the third-party certificate, then verify the issuing component's binding chain and the signature itself; nothing checked that the issuing component carried the RFC 9580 sec. 5.2.3.29 certification key flag (CERTIFY_OTHER) when the signature was created. A subkey bound only with SIGN_DATA - the online signing subkey of exactly the offline-primary arrangement those key flags exist to express - could therefore issue a positive User ID certification over an attacker-controlled identity, or a full-trust depth-one direct-key delegation of introducer trust, and the API returned it as a valid signature chain attributed to the third-party certificate. An application treating getCertificationBy(...).isValid() or getDelegationBy(...) as an identity or trusted-introducer decision would attribute the attacker's assertion to the offline primary key. The same held for a legacy RSA subkey bound only for encryption, whose algorithm is nonetheless able to sign. This does not forge the primary key's signature or recover any private key; it promotes an already-compromised restricted subkey to the primary key's identity-issuing authority, defeating the containment the key-flag separation provides. A third-party certification or delegation is now attributed to the issuing certificate only when the component key that made it is the primary key, or is a subkey holding CERTIFY_OTHER when the signature was created, so certification-capable subkeys continue to be accepted; primary keys are accepted whatever their key flags say, since a primary key is certification-capable by construction and certificates carrying no key flags subpacket at all are common. Third-party revocations are deliberately outside the rule, since declining to honour one would keep trust alive rather than withdraw it.	N/A	More Details
	In Bouncy Castle for Java before 1.86, the Messaging Layer Security (MLS, RFC 9420) implementation did not bind an X.509 credential to a LeafNode's signature_key. LeafNode.verify() checked a leaf's signature against the signature_key carried in the leaf itself, while the credential's X.509 certificate chain was stored but never parsed or validated, so the end-entity certificate's public key was never required to match signature_key as RFC 9420 sec. 5.3 requires. A party could therefore present another party's certificate as its credential while signing the leaf, and the enclosing KeyPackage, with an		

CVE-2026-71885	unrelated key, and be accepted under that other party's identity through KeyPackage.verify() and the Group leaf-validation path. In a deployment that admits external commits without an independent credential-admission check, an unauthenticated attacker could be admitted under a victim's X.509 identity, evict the victim (resynchronization compares whole credentials rather than signing keys), derive the current epoch, decrypt subsequent group messages, and send messages accepted as the victim. TreeKEM.LeafNode now requires the end-entity certificate's subject public key, in the cipher suite's signature encoding, to equal signature_key for an X.509 credential and rejects the leaf otherwise, including an empty chain or a certificate whose key type does not match the cipher suite; certificate-chain and identity validation to a trust anchor remain the application's responsibility per RFC 9420 sec. 5.3.1. Deployments using only basic credentials are unaffected.	N/A	More Details
CVE-2026-71883	In Bouncy Castle for Java LTS before 2.73.13, the one-shot native packet ciphers for AES-CBC, CCM, CFB, CTR, GCM and GCM-SIV released the caller's key, IV and additional authenticated data arrays with JNI's ReleaseByteArrayElements in mode 0, which commits the native copy back into the Java array. Those arrays are read-only to the native code, and on a JVM that returns a copy rather than a pin the copy still holds the input bytes as they were read. The output buffer is taken through a separate critical region and committed first, so where an application passed the same Java array as both an input and the destination - encrypting in place over KeyParameter.getKey(), for example - the later mode-0 release of the key wrote the unchanged key bytes over the ciphertext that had just been produced. The call still returned the correct output length, so an application encrypting in place over its own key array was handed the raw AES key where it expected ciphertext, with nothing in the API to indicate it, and would transmit or store the key in place of the message. The read-only input arrays are now released with JNI_ABORT, freeing the native copy without copying it back, and mode 0 is reserved for arrays the native code wrote. The pure-Java packet ciphers and the streaming native modes are not affected. Bouncy Castle for Java (bcprov) is not affected, as it ships no native implementations.	N/A	More Details
CVE-2026-18040	In Bouncy Castle for Java before 1.86, HQC leaked secret-derived data through two side channels: its GF(2^8) arithmetic used lookup tables indexed by field elements, making the cache line touched a function of the operand, and its fixed-weight support sampler left its duplicate scan as soon as a collision was found and stored accepted positions at a secret index. Both run on secret inputs during encapsulation and decapsulation, and the sampler re-expands the secret key from its seed on every decapsulation, so an attacker able to observe cache behaviour or decapsulation timing can recover information about the HQC private key. The field arithmetic is now table-free and the sampler branch-free within a batch of candidates, with output and randomness consumption unchanged.	N/A	More Details
CVE-2026-103656	Rejected reason: this is rejected	N/A	More Details
CVE-2026-103659	MISP contains an authorization bypass in the event flattening feature. When a user requests an event with the flatten option enabled, the application removes the Object containment from the query and returns object attributes as top-level event attributes. In doing so, the object-level distribution and sharing-group access control check was not re-applied to those attributes. As a result, a user who can view a community-distributed event could retrieve attributes belonging to organisation-only objects (distribution level 0) or objects restricted to a specific sharing group, even though the user's organisation does not have access to those objects. This constitutes an unauthorized disclosure of sensitive threat intelligence data. A secondary issue was introduced by the initial remediation: the fix reused the full Object contain conditions (including soft-delete state) as the gate for flattened attributes, causing an event owner requesting deleted attributes to lose all attributes whose parent object was still live. The final fix isolates the distribution ACL condition as the sole gate. Preconditions: - An authenticated user with access to a community-distributed event - The event contains at least one object with a distribution level or sharing group that restricts access beyond the event's own distribution Impact: - Unauthorized disclosure of attributes belonging to restricted objects - Potential exposure of organisation-specific threat intelligence to other organisations Affected versions: <2.5.48	N/A	More Details
CVE-2026-103662	MISP contains a reflected cross-site scripting (XSS) vulnerability in the legacy taxonomy tag management confirmation forms (add tag and disable tag). The affected forms echoed a user-supplied tag name value from the request unescaped into the rendered HTML output. An attacker who can induce a site administrator to visit a crafted URL containing a malicious tag name parameter can execute arbitrary JavaScript in the administrator's browser session. Preconditions: - The target must be running a MISP instance with the legacy taxonomy tag confirmation views enabled. - The victim must be an authenticated site administrator. - The victim must navigate to the attacker-crafted URL (e.g., via a phishing link). Security impact: - Execution of arbitrary client-side script in the context of the administrator's browser. - Potential theft of session tokens, CSRF tokens, or other sensitive data accessible from the page. - Potential for performing privileged actions on behalf of the administrator within the MISP interface. Affected versions: <2.5.48.	N/A	More Details
	MISP contains a reflected cross-site scripting (XSS) vulnerability in the analyst data notes panel. The		

CVE-2026-103664	seed path parameter, supplied by the user via the URL, was passed directly into inline JavaScript within the rendered HTML response without any sanitization or type enforcement. An attacker who can convince an authenticated MISP user to navigate to a crafted URL (for example, via a phishing link) can inject arbitrary JavaScript that executes in the victim's browser context. This may allow the attacker to read session tokens, manipulate the page, or perform actions on behalf of the victim. Preconditions: - The victim must be authenticated to MISP and access the analyst data view for an attribute or object. - The attacker must supply a malicious seed value in the URL path. Impact: - Execution of arbitrary JavaScript in the victim's browser session. - Potential theft of session credentials or sensitive data visible in the page. - Manipulation of the analyst data interface. Affected: MISP versions prior to the fix (commit 58925dbf0, post v2.5.48).	N/A	More Details
CVE-2026-34189	Cross-Site Request Forgery (CSRF) vulnerability allows unauthorized deletion of event responses via a forged GET request when an authenticated administrator visits a malicious page. This issue affects Pandora FMS: from 777 onwards.	N/A	More Details
CVE-2026-34190	Cross-Site Request Forgery (CSRF) vulnerability allows unauthorized deletion of alert commands via sequential, unvalidated GET requests when an authenticated administrator visits a malicious page. This issue affects Pandora FMS: from 777 onwards.	N/A	More Details
CVE-2026-64946	A chained CSRF and unrestricted SVG file upload vulnerability in the File Manager module allows stored Cross-Site Scripting, enabling session cookie exfiltration and administrator account takeover. This issue affects Pandora FMS: from 777 onwards.	N/A	More Details
CVE-2026-76142	Insufficient authentication and access control on the internal-only IPC SOAP endpoint of the Genian NAC/ZTNA policy server allows an unauthenticated attacker to invoke internal functions	N/A	More Details
CVE-2026-105206	ZITADEL 3.0.0 through 3.4.15 and 4.x before 4.17.3 contains an incorrect authorization flaw in the User Service API, which verifies user.read against the caller's organization rather than the organization owning the target user. An authenticated member holding org-scoped user.read can query GET /v2/users/{userId}/authentication_methods to learn which authentication method types users in other organizations have registered.	N/A	More Details
CVE-2026-64948	Missing authorization in module data retrieval allows unauthorized cross-group access to module history. Affects Pandora FMS from 777 onwards.	N/A	More Details
CVE-2026-14157	Use of an Externally Controlled Format String in the ASUS Router modules allow a remote authenticated user to execute arbitrary commands via a crafted file uploaded through the web management interface.	N/A	More Details
CVE-2026-80490	Algorithm::AhoCorasick::XS versions through 0.04 for Perl read the haystack string length before the scalar is stringified. The matches, first_match and match_details methods use the T_STD_STRING typemap to translate Perl scalars (SVs) into strings via the std::string constructor, using the SvPV macro to stringify the haystack input, and the SvCUR macro to determine the length of the SV. When the input SVs are references, integers (IVs) or floats (NVs), the SvCUR macro will return an invalid length if it is run before the input is stringified, leading to an out-of-bounds read which can abort the process. Note that the evaluation order of arguments to std::string is unspecified. Depending on the compiler, SvCUR may be run first and lead to an abort that cannot be caught within Perl. This can be triggered when the haystack is a numeric value, for example, my \$ac = Algorithm::AhoCorasick::XS->new(["11", "22"]); \$ac->matches(211); This can occur when the haystack is the result of reading data from decoded JSON or a numeric database column. It can also be triggered when using a blessed object as a haystack.	N/A	More Details
CVE-2026-103443	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki Collection (Book) extension allows XSS Targeting Non-Script Elements. This issue affects MediaWiki Collection (Book) extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-103444	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki WikiForum extension allows Stored XSS. This issue affects MediaWiki WikiForum extension: master.	N/A	More Details
CVE-2026-19445	A remote, unauthenticated TLS client can make a server crash or call through a freed pointer if its sni_callback assigns a different context to SSLSocket.context (the documented way to select a certificate per server name) and nothing else keeps the original ssl.SSLContext alive. Typical cases are servers that create an SSLContext per connection or replace it while connections are open; servers that wrap their listening socket with it are not affected. Mitigation: keep a reference to every SSLContext that sets sni_callback for the lifetime of the server. TLS clients are not affected.	N/A	More Details
	ssl.SSLContext.wrap_bio() didn't require the server_hostname argument to not be None if		

CVE-2026-19553	ssl.SSLContext.check_hostname was set. Due to a missing parameter check in SSLObject, if the server_hostname argument isn't supplied then hostname verification would be silently skipped. This defect could lead to programs where certificate hostname verification *appeared* to be succeeding with SSLContext.check_hostname = True and no ValueError being raised due to misconfiguration. If the program passes a server_hostname value that isn't an empty string or None to any of these APIs then certificate hostname verification proceeds as expected and the program is not affected by this vulnerability. Mitigating this vulnerability doesn't require updating Python or applying the patch. To mitigate, pass a valid non-None and non-empty server_hostname value to SSLContext.wrap_bio(), asyncio.create_connection(), or asyncio.loop.start_tls() and certificate hostname verification will proceed as expected. Upgrading to the latest version of Python or applying the patch only changes the behavior from silently skipping hostname verification to raising a ValueError, similar to SSLContext.wrap_socket(), when server_hostname isn't supplied.	N/A	More Details
CVE-2026-55177	CloudTAK is a browser-based Common Operating Picture and situational awareness tool compatible with TAK. Prior to version 13.10.0, every route in the ESRI helper family (api/routes/esri.ts) takes a fully attacker-controlled URL from the request (POST /api/esri body url, and the portal / server / layer query parameters on the GET /api/esri/* routes) and passes it into EsriBase / EsriProxyPortal / EsriProxyServer / EsriProxyLayer in api/lib/esri.ts, which fetch it with the bare fetch from @tak-ps/etl. No IP / DNS / hostname classification is applied at any point, so the destination is never validated against private, loopback, or link-local ranges. Any authenticated user (the routes only require Auth.is_auth(config, req, { anyResources: true })), i.e. any token, not an admin) can therefore make the CloudTAK server issue arbitrary outbound GET/POST requests to internal addresses such as the cloud instance-metadata service (169.254.169.254), loopback admin ports (127.0.0.1:<port>), and other hosts reachable only from inside the deployment VPC. This is a full-read SSRF, not blind: on success the upstream JSON body is returned to the caller via res.json(...), and on failure the upstream error string is reflected verbatim as ESRI Server Error: <message>. An attacker can read cloud metadata (and the temporary IAM credentials the instance role exposes), enumerate internal services, and exfiltrate their response bodies. The sniff() URL classifier provides no protection: it only pattern-matches the pathname (/rest, /arcgis/rest, /sharing/rest), so a URL like http://169.254.169.254/arcgis/rest or http://127.0.0.1:8500/rest passes sniff() and is fetched. This issue has been patched in version 13.10.0.	N/A	More Details
CVE-2026-75969	Missing authentication for critical function vulnerability for all PTZOptics cameras and the Firmware Upgrade Tool - Firmware Update modules. A missing authentication vulnerability in the firmware update mechanism of affected PTZOptics cameras allows an unauthenticated user to install modified firmware on the device without administrator credentials. This vulnerability allows attackers to upload modified firmware to the device without admin credentials. This issue affects: * Move 4K 12X before: 0.0.98 * Move 4K 20X before: 0.1.33 * Move 4K 30X before: 2.1.17 * Link 4K 12X before: 0.0.99 * Link 4K 20X before: 0.1.37 * Link 4K 30X before: 2.1.18 * Move SE 12X before: 9.1.66 * Move SE 20X before: 9.1.44 * Move SE 30X before: 9.1.46 * Studio 4K 12X before: 8.3.32 * Studio 4K 20X before: 8.3.32 * Studio SE 12X before: 8.3.32 * Studio SE 20X before: 8.3.32 * All Generation 2 cameras, including: PT12X-SDI-GY-G2, PT12X-SDI-WH-G2, PT12X-NDI-GY-G2, PT12X-NDI-WH-G2; PT12X-USB-GY-G2, PT12X-USB-WH-G2; PT20X-SDI-GY-G2, PT20X-SDI-WH-G2, PT20X-NDI-GY-G2, PT20X-NDI-WH-G2; PT20X-USB-GY-G2, PT20X-USB-WH-G2; PT30X-SDI-GY-G2, PT30X-SDI-WH-G2, PT30X-NDI-GY-G2, PT30X-NDI-WH-G2; PTVL-ZCAM, PTVL-NDI-ZCAM; PTEPTZ-ZCAM-G2, PTEPTZ-NDI-ZCAM-G2; PT12X-ZCAM, PT12X-NDI-ZCAM; PT20X-ZCAM, PT20X-NDI-ZCAM; Studio Pro - All versions * Upgrade Tool - All versions	N/A	More Details
CVE-2026-103437	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki ReadingLists extension allows Reflected XSS. This issue affects MediaWiki ReadingLists extension: 1.46 and 1.45.	N/A	More Details
CVE-2026-103438	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki Wikistories extension allows Cross-Site Scripting (XSS). This issue affects MediaWiki Wikistories extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-103439	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki Wikibase extension allows Cross-Site Scripting (XSS). This issue affects MediaWiki Wikibase extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-103440	Exposure of sensitive information through data queries vulnerability in The Wikimedia Foundation MediaWiki PageTriage extension allows Information Elicitation. This issue affects MediaWiki PageTriage extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-103445	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki Page_Forms extension allows Stored XSS. This issue affects MediaWiki Page_Forms extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-103446	Authorization bypass through User-Controlled key vulnerability in The Wikimedia Foundation MediaWiki WikiLambda extension allows Authentication Bypass. This issue affects MediaWiki WikiLambda extension: 1.46.	N/A	More Details

CVE-2026-103500	An attacker could cause a heap buffer overflow by getting a user to open an email that is greater than or equal to 2GB in size. This vulnerability was fixed in Thunderbird 157, Thunderbird 140.17, and Thunderbird 153.4.	N/A	More Details
CVE-2026-55094	Taskcluster is the task execution framework that supports Mozilla's continuous integration and release processes. Prior to version 100.3.0, Taskcluster is vulnerable to unauthenticated RCE on Taskcluster deployments with an anonymous role that exposes the GraphQL endpoint and parses filter arguments using the sift library. This issue has been patched in version 100.3.0.	N/A	More Details
CVE-2026-55224	MineAdmin is a ready-to-use backend management system suitable for quickly building website backends, operation platforms, permission centers, internal management systems, CMS, CRM, OA, ERP and other business applications. Prior to version 3.2.0-alpha.2, the app-store plugin service concatenates unsanitized user-supplied identifier values directly into file system paths. An attacker can use path traversal sequences (e.g., ../) to read, install, or uninstall plugins from arbitrary directories, and potentially execute arbitrary composer commands. This issue has been patched in version 3.2.0-alpha.2.	N/A	More Details
CVE-2026-102990	basic-ftp is an FTP client for Node.js. Prior to 6.2.1, Client.list() can be forced by a malicious or compromised FTP server to spend quadratic CPU time parsing a directory listing because the RE_LINE expression in src/parseListUnix.ts backtracks across adjacent variable-length owner and group fields when a long Unix-style line has a valid prefix but cannot satisfy the later size and date fields. parseList() selects a parser from the last nonblank line and then applies it to every line, so a normal final line can select the Unix parser while an earlier crafted line blocks the Node.js event loop and freezes the process. This issue is fixed in version 6.2.1.	N/A	More Details
CVE-2026-102992	piscina is a node.js worker pool implementation. Prior to 4.9.4, 5.3.2, and 6.0.0-rc.5, Piscina stores ThreadPool.options in src/index.ts as a plain object that inherits from Object.prototype. Applications with a separate prototype-pollution primitive can therefore supply inherited values for security-sensitive options that do not have own defaults. An inherited execArgv value is passed to the Node.js Worker constructor and can preload attacker-controlled code in worker threads, an inherited loadBalancer function can execute during task scheduling, and inherited env values can alter worker environments. This issue is fixed in versions 4.9.4, 5.3.2, and 6.0.0-rc.5.	N/A	More Details
CVE-2026-103547	In ldapd in OpenBSD 7.8 before errata 057 and 7.9 before errata 021, delegated BSD authentication results are correlated only by the LDAP child process client file descriptor and LDAP message ID. After a connection closes, a later connection that reuses the same file descriptor and message ID can receive the earlier authentication result. A remote attacker who can reach ldapd can complete a Bind as another identity. A missing connection can also cause a NULL pointer dereference. (ldapd is not enabled by default.)	N/A	More Details
CVE-2026-103548	Improperly stored passwords in the config file in Itron MV-90 xi 3.0 allows attackers to decode the passwords and password histories to gain access to the MV-90 application as any user.	N/A	More Details
CVE-2026-101276	iperf3 3.21 (esnet/iperf) contains a remote, unauthenticated heap use-after-free: the server's per-test watchdog server_timer_proc() frees streams without cancelling/joining their worker threads, so a blocked worker dereferences a freed iperf_stream; fixed in 3.22.	N/A	More Details
CVE-2026-51852	agent-zero 1.7, 1.8, 1.9, and 1.10 is vulnerable to Directory Traversal in python/helpers/file_browser.py:FileBrowser.save_file_b64. The save_file_b64 method accepts user-controlled file paths without normalization or validation, allowing path traversal attacks.	N/A	More Details
CVE-2026-51862	DB-GPT 0.8.0 contains directory traversal in skill_upload (packages/dbgpt-app/src/dbgpt_app/openapi/api_v1/agent_data_api.py:40). A remote attacker can use the validated exploitation path to write files outside the intended workspace or storage boundary.	N/A	More Details
CVE-2026-51869	DB-GPT v0.8.0 sandbox API silently falls back to LocalRuntime and executes code on host.	N/A	More Details
CVE-2026-101283	iperf3 3.20-3.21 (esnet/iperf) has a pre-auth heap buffer overflow in decrypt_rsa_message(): a 256-byte RSA buffer is BIO_read with the attacker-controlled ciphertext length (guard warns only), so an unauthenticated client overflows the heap via an oversized authtoken; fixed in 3.22	N/A	More Details
CVE-2026-103584	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The Wikimedia Foundation MediaWiki CommonsMetadata extension allows Cross-Site Scripting (XSS). This issue affects MediaWiki CommonsMetadata extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in The		

2026-103585	Wikimedia Foundation MediaWiki MediaSearch extension allows Cross-Site Scripting (XSS). This issue affects MediaWiki MediaSearch extension: 1.46, 1.45, and 1.43.	N/A	More Details
CVE-2026-105214	Zitadel before 4.16.2 contains a server-side request forgery vulnerability that allows attackers to make the server request internal resources through organization domain HTTP verification. The challenge fetch uses Go's default http.Get instead of the protected client, so attackers can register domains that redirect to loopback, internal, or cloud metadata addresses to scan ports and map internal networks.	N/A	More Details
CVE-2026-13313	An Active Debug Code vulnerability in certain ASUS router models allows a remote authenticated user, via a crafted HTTP request, to bypass security mechanisms and enable the Telnet service, thereby executing arbitrary commands with root privileges and potentially affecting other devices connected to the router. Refer to the ' Security Update for ASUS Router Firmware ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-64947	A chained CSRF bypass and unrestricted file upload vulnerability in the Plugin File Manager allows an attacker to upload and execute arbitrary PHP code, resulting in Remote Code Execution. This issue affects Pandora FMS: from 777 onwards.	N/A	More Details
CVE-2026-64949	Incomplete extension blacklist in the File Manager module allows authenticated upload and execution of arbitrary .phar files. Affects Pandora FMS from 777 onwards.	N/A	More Details
CVE-2026-96277	Uncaught exception, Improper Handling of Exceptional Conditions vulnerability in Apache Thrift Ruby bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-104853	Nx is a monorepo solution for TypeScript and polyglot codebases. From 13.10.0 until 22.7.10 and 23.2.1, Nx migration planning reads the nx-migrations.migrations value from a target package manifest without validating that it is a contained relative path. A hostile direct dependency or a package introduced through a trusted package's packageGroup can supply .. segments or an absolute path, causing nx migrate to join an escaping destination onto its temporary directory. The migration archive can then write attacker-controlled bytes outside the temporary directory, while opening the destination stream can truncate an existing writable file even when no archive entry matches. This occurs during migration planning before review of the migration list or use of --run-migrations; the vulnerable installed Nx copy is reached when the normal nx@latest handoff is bypassed with NX_USE_LOCAL, NX_MIGRATE_USE_LOCAL, NX_MIGRATE_CLI_VERSION, --run-id, or fallback after a temporary-install failure. This issue is fixed in versions 22.7.10 and 23.2.1.	N/A	More Details
CVE-2026-104849	Tinypool is a minimal Node.js worker thread pool implementation. Prior to 2.1.2, Tinypool reads filename from a caller-supplied options object in pool.run(task, options) without requiring an own property, so a polluted Object.prototype.filename can replace the intended worker module. Applications are affected only when they pass their own second-argument options object to pool.run(); calls without that argument use the trusted default options object. An attacker who can first pollute the prototype can cause the worker pool to load attacker-selected JavaScript and can read or modify task data with the host process's privileges. This issue is fixed in version 2.1.2.	N/A	More Details
CVE-2026-104848	Tinypool is a minimal Node.js worker thread pool implementation. Prior to 2.1.1, Tinypool constructs ThreadPool.options from a normal options object and reads the execArgv and env worker options in dist/index.js, allowing values inherited from a polluted Object.prototype to be copied into own properties and passed to worker_threads.Worker. An attacker who can first pollute either property can cause each newly spawned worker to load attacker-selected JavaScript through command-line preload arguments or NODE_OPTIONS, resulting in code execution with the host process's privileges and possible access to CI secrets, signing material, or build artifacts. This issue is fixed in version 2.1.1.	N/A	More Details
CVE-2026-73975	djehuty is a research data repository system developed by 4TU.ResearchData. Prior to version 26.3.2, an authenticated depositor can inject arbitrary SPARQL into a state-modifying (DELETE/INSERT) query by supplying a crafted session name, letting them write (and delete) arbitrary triples anywhere in the RDF store. Because the RDF store is shared across all accounts and datasets, this is an integrity compromise of the whole repository's metadata, not just the attacker's own records. Having a logged-in account is a precondition. djehuty allows self-registration via ORCID/SAML, so this is a low barrier in typical deployments. This issue has been patched in version 26.3.2.	N/A	More Details
CVE-2026-102294	TP-Link TL-WR841N contains an authenticated OS command injection vulnerability in the IPv6 WAN configuration. A crafted IPv6 Gateway value is improperly incorporated into a system command, allowing an authenticated administrator to execute arbitrary operating system commands. Successful exploitation may allow unauthorized access to sensitive information, modification of device configuration or services, and disruption of device operation.	N/A	More Details
	MISP contains an improper access control vulnerability in its attribute search and paginated attribute		

CVE-2026-104914	view endpoints. When a user queries for soft-deleted attributes (e.g., via the deleted-attributes search or the paginated attribute listing), the application returned soft-deleted attributes belonging to events owned by other organizations to any authenticated user who had visibility of the event. The event detail view correctly restricted soft-deleted attribute visibility to the owning organization and sync-permission users, but the attribute search and paginated view code paths lacked this restriction. Preconditions: - An authenticated MISP user with at least read access to an event owned by another organization. - The user issues a query for deleted attributes (search or paginated view with the deleted filter). Impact: - Confidentiality: Soft-deleted threat intelligence attributes (e.g., IOCs, indicators, context) from other organizations are disclosed to unauthorized users. This may expose sensitive intelligence that the owning organization intended to remove from general visibility. Affected versions: MISP versions prior to v2.5.48.	N/A	More Details
CVE-2026-104912	MISP contains an authorization flaw in its correlation handling during attribute searches. When a user performs an attribute search that triggers correlation lookups, the system authorized access to correlated attributes and events based on a stale distribution snapshot stored on the correlation row rather than the live event access control list. Because the correlation row's distribution columns are a point-in-time copy that lacks a published flag, the authorization check becomes incorrect when an event is subsequently restricted (for example, its sharing group is changed or it is unpublished). As a result, an authenticated user could retrieve attributes and event details belonging to events they no longer have permission to view. Preconditions: - An authenticated user with at least read access to some events in the instance. - The existence of correlations between events, at least one of which has been restricted after the correlation was created. Impact: - Confidentiality: exposure of attribute values and event metadata that the user is not authorized to access. Affected versions: MISP prior to v2.5.48.	N/A	More Details
CVE-2026-104910	MISP contains an authorization bypass in the related events listing functionality. When a user requests the list of events correlated to a given event, the system retrieved related event metadata directly from the correlation table without re-validating the caller's access rights against each related event. The correlation table stores a snapshot of the event's distribution level and sharing group at the time the correlation was created, and does not carry the published flag. As a result, events that the caller is not permitted to open—because they are unpublished, or because their distribution or sharing group has changed since the correlation was recorded—were still returned with their metadata (title, date, correlating value counts). Preconditions: - An authenticated user with access to at least one event in MISP. - The existence of correlation entries linking that event to other events the user should not be able to view. Impact: - Unauthorized disclosure of event metadata (titles, dates, correlation counts) for events the user has no right to access. - Potential reconnaissance of threat-intelligence event names and timelines across sharing groups. Affected: MISP versions prior to the fix commit (2ffa97f05).	N/A	More Details
CVE-2026-104908	MISP contains an improper input validation vulnerability in the decaying model import functionality. The import endpoint was intended to create a new decaying model belonging exclusively to the importing user's organisation, with the default flag forced to off. However, the application stripped only the top-level id and uuid fields and pinned org_id and default on the outer array before saving the data flat. A user with decaying-model permissions could supply a nested model key carrying its own primary key, organisation identifier, and default flag, which bypassed those guards during the save operation. Impact: - A user with perm_decaying could overwrite an existing decaying model belonging to another organisation in place, altering its name, formula, parameters, or ownership. - A user could create or modify a model flagged as the organisation default, affecting scoring behaviour for other users. - A user could reassign a model's organisation to an arbitrary value. Preconditions: - Authenticated user with decaying-model permission (perm_decaying). - Network access to the MISP instance. Affected: <2.5.48.	N/A	More Details
CVE-2026-104907	MISP contains a cross-site scripting (XSS) vulnerability in the remote event preview page. When a linked (remote) MISP server is configured, the event preview renders tag identifiers inside an inline JavaScript onclick attribute. The tag ID value was HTML-escaped but not sanitized for the JavaScript string context, meaning a malicious linked server could supply a tag ID containing characters (such as a single quote) that break out of the JavaScript string literal and inject arbitrary script. Preconditions: - A linked/remote MISP server is configured and connected to the local instance. - The linked server supplies a crafted tag ID in an event. - An authenticated user views the event preview and interacts with the affected tag element. Impact: - Arbitrary JavaScript execution in the context of the viewing user's browser session, potentially allowing session hijacking, data exfiltration, or unauthorized actions on behalf of the user. Affected versions: MISP prior to the fix commit (v2.5.48 or later, exact boundary unconfirmed).	N/A	More Details
CVE-2026-104906	MISP contains a cross-site scripting (XSS) vulnerability in the TAXII object viewer. When displaying a remote TAXII object, the JSON content of string properties was rendered directly into an HTML pre block without HTML-encoding. An attacker who can control or influence the content of a TAXII object (e.g., by publishing a malicious object to a TAXII server that the victim's MISP instance subscribes to) can inject arbitrary HTML or JavaScript that executes in the context of the victim's MISP session. Preconditions: - The victim must be an authenticated MISP user with access to the TAXII object viewer. - The victim must open or view the crafted TAXII object. Impact: - Execution of arbitrary JavaScript in the victim's	N/A	More Details

	browser within the MISP application context. - Potential theft of session tokens, API keys, or other sensitive data accessible from the MISP interface. - Potential for performing actions on behalf of the authenticated user. Affected versions: <2.5.48.		
CVE-2026-104901	MISP contains a cross-site scripting (XSS) vulnerability in the ID Translator feature. When a user views the ID Translator page, the application queries linked (remote) MISP servers for corresponding event identifiers. The event ID returned by the remote server was rendered in the HTML output without proper output encoding. A malicious or compromised linked server could return a crafted event ID containing arbitrary HTML or JavaScript markup. This markup would be rendered in the browser of any user in the host organization who views the ID Translator page, enabling session hijacking, credential theft, or other client-side attacks. Preconditions: - The victim must be an authenticated user of the host MISP instance. - A linked server must be configured on the host instance. - The victim must navigate to the ID Translator page for a given event. Affected versions: <2.5.48.	N/A	More Details
CVE-2026-104900	MISP contains a stored cross-site scripting (XSS) vulnerability in the index table rendering of the remote event preview. The count field template escaped the associated link URL but rendered the field value without HTML encoding. An attacker with the ability to create or modify events on a linked (remote) MISP server could craft an event identifier containing HTML or JavaScript markup. When a user on the local MISP instance views the remote event preview index, the unescaped value is rendered directly in the browser, allowing arbitrary script execution in the victim's session. Preconditions: - A linked/remote MISP server is configured and connected to the local instance. - The attacker has sufficient access on the linked server to create or modify an event with a crafted identifier. - A victim user on the local instance views the remote event preview index page. Impact: - Execution of arbitrary JavaScript in the context of the MISP web application. - Potential session hijacking, data exfiltration, or unauthorized actions performed on behalf of the authenticated user. Affected versions: <2.5.48.	N/A	More Details
CVE-2026-104847	ProseMirror's view component renders and manages the editable browser interface for ProseMirror documents. Prior to 1.42.3, prosemirror-view paste handling accepts attacker-provided HTML whose clipboard slice context contains attributes that are not passed through schema attribute validation. When a user pastes the crafted HTML into an editor, the unvalidated context attributes can construct content that executes attacker-controlled JavaScript in the browser window containing the editor. This issue is fixed in version 1.42.3.	N/A	More Details
CVE-2026-102369	Tapo C120 v1 and C200 V5 do not adequately protect login challenge data or sanitize attacker-controlled input processed by the MacTool handler. An unauthenticated attacker on the same local network can replay login challenge data to obtain an administrative session, enable a privileged service that becomes accessible after a reboot, and submit crafted input to execute arbitrary commands within the device management process. Successful exploitation may allow arbitrary command execution on the camera and compromise the confidentiality, integrity, and availability of the affected device. Exploitation requires access from the same local network, replay of the login challenge data, activation of the privileged service, and a device reboot.	N/A	More Details
CVE-2026-104843	uv is a Python package and project manager written in Rust. From 0.12.7 until 0.12.18, uv wheel extraction on Windows can process a malicious wheel in a way that writes a file outside the installation prefix, including an executable in a directory already present on the user's PATH. Non-Windows hosts are not affected. This issue is fixed in version 0.12.18.	N/A	More Details
CVE-2026-103923	KaTeX is a fast, easy-to-use JavaScript library for TeX math rendering on the web. From 0.11.0 until 0.18.2, KaTeX uses ordinary JavaScript property access for the renderer options object, the trust setting, default and processor setting metadata, and namespace lookup and group restoration, allowing inherited properties to be treated as explicitly supplied values. When Object.prototype is already polluted or an attacker controls the options object's prototype, attacker-controlled mathematical expressions can use an inherited trust value to enable trusted rendering and produce links capable of user-interaction cross-site scripting or loading attacker-selected external resources in a consuming application that inserts unsanitized KaTeX output into a page. KaTeX does not itself create the prototype pollution, and rendering an expression alone does not execute script. This issue is fixed in version 0.18.2.	N/A	More Details
CVE-2026-73976	djehuty is a research data repository system developed by 4TU.ResearchData. Prior to version 26.3.2, An unauthenticated attacker can inject SPARQL into the search/listing queries through three separate parameters. Because the affected queries are read (SELECT) queries, this does not write to the store, but it allows: Cross-graph data exfiltration — e.g. UNION-ing in triples from graphs the request was never scoped to (drafts/private/internal data held in the RDF store); denial of service — expensive or malformed queries that tie up the SPARQL backend / web workers. No account or user interaction is required. This issue has been patched in version 26.3.2.	N/A	More Details
CVE-	Tapo C120 v1 and C200 V5 contain a vulnerability in the HTTPS onboarding scan function due to missing authentication. After initial setup, an unauthenticated attacker on the same local network can		

2026-78577	invoke the scan action and retrieve nearby wireless access-point metadata, including SSIDs, BSSIDs, authentication and encryption modes, and signal-strength information. Successful exploitation may disclose information about the wireless environment surrounding the camera, allowing an attacker to learn elements of the local wireless topology.	N/A	More Details
CVE-2026-78578	Tapo C120 v1 and C200 v5 do not enforce authentication for do method HTTPS onboarding connect actions after initial setup. An unauthenticated adjacent attacker can submit unauthorized wireless configuration parameters, causing the camera to attempt connection to a different network. Successful exploitation disconnects the camera from its intended wireless network, making it unreachable on its management address, resulting in a denial-of-service condition.	N/A	More Details
CVE-2026-9032	Tapo C120 v1 and C200 v5 contain a NULL pointer dereference in the HTTPS onboarding connect request parser. The interface is reachable without authentication after initial setup and does not validate that a password field is present for certain authentication and encryption parameter combinations, allowing a malformed request from the same local network to crash the HTTPS service. Successful exploitation may temporarily make HTTPS management functions unavailable. Repeated malformed requests may sustain the denial-of-service condition, and recovery may in some cases require a device reboot.	N/A	More Details
CVE-2026-27872	- Improper Privilege Management vulnerability in Johnson Controls Easy IO FG allows (Brute Force). This issue affects Easy IO FG: before 2.0b52.	N/A	More Details
CVE-2026-63721	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-63724	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-84682	A command injection vulnerability exists in the TDDPv2 service (/usr/bin/tddp) on Archer AX90 V1. An unauthenticated adjacent-network attacker can exploit the setProductVer command handler to execute arbitrary operating system commands as root during device boot. Successful exploitation may result in complete device compromise through arbitrary command execution with root privileges.	N/A	More Details
CVE-2026-8618	A stack-based buffer overflow vulnerability exists in the TDDPv2 service (/usr/bin/tddp) on Deco M9 Plus due to insufficient validation of decrypted request data length before it is copied into a fixed-size stack buffer in the subtype 0x91 handler. Successful exploitation may allow an adjacent, unauthenticated attacker to cause a denial of service or achieve arbitrary code execution during the device setup phase through crafted TDDP packets.	N/A	More Details
CVE-2026-104721	Path-traversal vulnerability in QOS.CH Srl Logback-classic on Java (logback-classic module) allows path-traversal vulnerability. More specifically, an MDC-based discriminator value flows unsanitized into a nested FileAppender path, letting an attacker who influences that MDC value (e.g. via an HTTP header) create and append log files outside the intended directory. This issue affects Logback-classic: from 0.9.14 through 1.6.4. This vulnerability is similar to CVE-2026-19880 but involves other attack techniques.	N/A	More Details
CVE-2026-96289	Uncontrolled Recursion vulnerability in Apache Thrift PHP bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-96287	Inefficient Algorithmic Complexity vulnerability in Apache Thrift Perl bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-96286	Uncaught exception vulnerability in Apache Thrift Perl bindings. This issue affects Apache Thrift: before 0.25.0. Users are recommended to upgrade to version 0.25.0, which fixes the issue.	N/A	More Details
CVE-2026-13043	A missing authentication vulnerability in the Kernel Memory Access Driver (PSKMAD) used by WatchGuard endpoint security products allows a local, authenticated attacker to bypass the driver's access-control handshake and issue arbitrary privileged commands to the driver, resulting in disclosure of kernel and process memory.	N/A	More Details
CVE-	Nx is a monorepo solution for TypeScript and polyglot codebases. From 14.6.0 until 22.7.9 and 23.1.2, Nx creates Unix domain sockets for its daemon and isolated plugin workers in shared temporary locations without owner-only directory and socket permissions. Another unprivileged local account on a shared build server, developer host, or multi-user container can discover and connect to a running		

2026-104854	socket because the transport performs no authentication and relies on filesystem containment. The daemon's PROCESS_IN_BACKGROUND request accepts a module path and invokes its default export, allowing a caller that controls a file to execute code as the account running Nx; other handlers can expose workspace file contents, project graphs, and task hashes. Disabling the daemon alone does not remove the vulnerable plugin-worker sockets, while single-user machines without another local account are not exposed. This issue is fixed in versions 22.7.9 and 23.1.2.	N/A	More Details
CVE-2026-64950	Missing input validation and output encoding on the directory name parameter in File Manager's Create Directory allows stored XSS, executing without user interaction. Affects Pandora FMS from 777 onwards.	N/A	More Details
CVE-2026-102626	An authenticated LimeSurvey Community Edition 7.4.0 user with the global Surveys: create permission can store a JavaScript-breaking value in the date_min attribute of a Date/Time question. When another user renders the affected question, LimeSurvey inserts the stored value into a single-quoted inline JavaScript literal without JavaScript-context encoding.	N/A	More Details
CVE-2026-75786	Unsanitized concatenation of the module parameter in the Grafana datasource endpoint allows authenticated blind SQL injection. Affects Pandora FMS from 777 onwards.	N/A	More Details
CVE-2026-7173	CVE-2026-7173: Cross-Site Scripting vulnerability in Entradium, by Crocantickets. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to the victim and steal their session data. * (Stored XSS) The City parameter in the endpoint /events/<event_name>/edit_general during the process of creating or editing events assigned to a promoter allows for the injection of JavaScript that will execute on the event's public page. * (Reflected XSS) The Description parameter in the endpoint /events/<event_name>/edit-general when attempting to create or modify an event without filling in all required fields.	N/A	More Details
CVE-2026-7174	CVE-2026-7174: Stored Cross-Site Scripting vulnerability in Entradium, by Crocantickets. Specifically, in the Name and Field parameters of the endpoint /tools/discount_wizard/discount_config during the process of creating discounts assigned to an event. This vulnerability allows JavaScript code to be injected into the affected parameters, which executes when an event's discount list page is displayed. Successful exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to the victim and steal their session data.	N/A	More Details
CVE-2026-7175	CVE-2026-7175: the Business Name parameter in the /promoters/edit endpoint of the My Profile section of a promoter's profile, which allows the injection of JavaScript code that will execute on the promoter's public page;	N/A	More Details
CVE-2026-7176	CVE-2026-7176: the Help text and Title parameters in the endpoint /events/<event_name>-<event_city>/custom_form/edit during the process of creating or modifying forms associated with ticket sales for an event, which allows for the injection of JavaScript that will execute on the public ticket purchase page for the event.	N/A	More Details
CVE-2026-78242	Insertion of sensitive information into log file vulnerability in Apache APISIX. This vulnerability can cause the unmasked header value to be written to the log sink under a certain response structure. This issue affects Apache APISIX: 3.17.0. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	N/A	More Details
CVE-2026-82806	Exposure of data element to wrong session vulnerability in Apache APISIX. This issue affects Apache APISIX: from 2.3.0 before 3.7.0. Under a supported authz-keycloak configuration, a request's authorization scope could persist into later requests on the same route, leading to unintended authorization expansion and inconsistent access-control decisions. Users are recommended to upgrade to version 3.7.0 or higher, which fixes the issue.	N/A	More Details
CVE-2026-103858	MISP contains an incomplete authorization check in the discussion posting functionality. When a user submits a post to a thread or replies to an existing post, the application only verified whether the target thread was restricted to a single organization (org-only distribution). It did not enforce the full thread access control list, including sharing-group membership and event-level visibility. As a result, an authenticated user who is outside the relevant sharing group or who does not have visibility on the associated event could: - Read the thread title and the content of the quoted post - Submit a new post into the discussion thread This constitutes both an information disclosure (reading restricted thread and post content) and an integrity issue (injecting content into a thread the user is not authorized to participate in). Affected: <2.5.48	N/A	More Details
CVE-2026-94212	Improper verification of cryptographic signature vulnerability in Apache APISIX. Any unauthenticated attacker could impersonate any user on every route protected by the saml-auth plugin under default configuration. This issue affects Apache APISIX: from 3.17.0 through 3.18.0. Users are recommended to upgrade to version 3.19.0, which fixes the issue.	N/A	More Details

CVE-2026-94220	Cross-Site request forgery (CSRF) vulnerability in feishu-auth and dingtalk-auth plugins in Apache APISIX. An attacker who can get a user to click a crafted link may cause that user's browser session on a protected route to be established under the attacker's identity instead of their own. Any work the user then performs in that session, including uploads, form submissions, and account bindings, lands in the attacker's account. This issue affects Apache APISIX: from 3.17.0 through 3.18.0. Users are recommended to upgrade to version 3.19.0, which fixes the issue.	N/A	More Details
CVE-2026-94250	Allocation of resources without limits or throttling vulnerability in batch-requests plugin in Apache APISIX. An unauthenticated caller can drive a gateway worker into OOM via a route where the batch-requests plugin is used and the batch endpoint is publicly exposed. This issue affects Apache APISIX: from 1.3.0 through 3.18.0. Users are recommended to upgrade to version 3.19.0, which fixes the issue.	N/A	More Details
CVE-2026-94269	Use of Non-Canonical URL paths for authorization decisions vulnerability in Apache APISIX. In some configurations where a permissive route overlaps a protected one, a crafted encoded path can reach an upstream endpoint that the matched route's policies were never meant to cover. A request that should have been rejected is served instead, giving unauthenticated access to a protected upstream endpoint. This issue affects Apache APISIX: from 2.14.1 through 3.18.0. Users are recommended to upgrade to version 3.19.0, which fixes the issue.	N/A	More Details
CVE-2026-94276	Improper Authentication vulnerability in Apache APISIX. On a route using openid-connect plugin with remote introspection against an authorization server that serves multiple issuers, a token that introspects as active for one issuer may get accepted on a route restricted to another. This issue affects Apache APISIX: from 3.12.0 through 3.18.0. Users are recommended to upgrade to version 3.19.0, which fixes the issue.	N/A	More Details
CVE-2026-105090	Formbricks before 5.4.4 and 6 before 6.0.1 allows stored XSS. The survey-level Custom Head Scripts feature did not enforce the documented Manage permission boundary. A workspace member holding only readWrite permission could configure Custom Head Scripts on a survey, an operation the documentation restricts to the Manage role. Because the configured scripts execute in the authenticated browser session of any user who opens the affected survey, a lower-privileged member can run arbitrary JavaScript (stored cross-site scripting) in the session of higher-privileged users. Fixed versions require Manage access to modify survey Custom Head Scripts.	N/A	More Details
CVE-2026-79113	OpenAPV before 1.1.1.0 has a read_bitstream heap-based buffer overflow.	N/A	More Details
CVE-2026-105050	PeaZip before 11.3.0, in a non-default configuration, is vulnerable to OS command injection via a filename in an archive because "quotation character already used in the string" is mishandled.	N/A	More Details
CVE-2026-104887	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-78409. Reason: This candidate is a duplicate of CVE-2026-78409. Notes: All CVE users should reference CVE-2026-78409 instead of this candidate	N/A	More Details
CVE-2026-104886	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-78410. Reason: This candidate is a duplicate of CVE-2026-78410. Notes: All CVE users should reference CVE-2026-78410 instead of this candidate	N/A	More Details
CVE-2026-75937	A specially crafted HTTP POST request to the web administration interface allows an unauthenticated attacker to execute arbitrary operating system commands with root privileges on the affected device. Disable the web server when not configuring the device.	N/A	More Details
CVE-2026-104055	The postgresql-operator charm runs a Prometheus postgres_exporter to collect database metrics using a dedicated "monitoring" PostgreSQL user. On database connection errors, the exporter writes the monitoring user's password in cleartext to its logs. Any actor able to read those logs can recover the password, which grants read-only pg_monitor access to PostgreSQL. This is fixed in the dev track (14/edge) in revisions 1189 (arm64) and 1190 (amd64), and in the stable track (14/stable) in revisions 1216 (arm64) and 1217 (amd64).	N/A	More Details
CVE-2026-104873	LangGraph Python SDK is used to connect to running LangGraph API servers, manage assistants, threads and stream runs from Python applications. From 0.1.45 until 0.4.4, the langgraph-sdk resource-scoped authorization decorators @auth.on.threads, @auth.on.assistants, and @auth.on.crons ignore the actions argument and register the selected handler for every action on the resource. Because that wildcard resource handler is selected before broader fallback handlers, an authenticated user may bypass fallback action, ownership, or permission checks and read, update, or delete another user's resource. Only Python deployments using actions on the affected decorators are vulnerable, and a deployment remains protected when the selected handler independently enforces all required checks for every action it receives. This issue is fixed in version 0.4.4.	N/A	More Details

CVE-2026-104871	The Angular SSR is a server-side rendering tool for Angular applications. Prior to versions 20.3.36, 21.2.23, and 22.1.7, the CommonEngine retrieveSSGPage prerendered-page retrieval logic in @angular/ssr/node, and in @angular/ssr for versions 17 through 18, accepts a relative request URL containing a backslash parent-traversal segment on Windows. The non-special resolve:// URL base preserves the backslash, path.join interprets it as a Windows separator, and the pagePath.startsWith(normalize(publicPath)) check incorrectly accepts a sibling output directory whose name shares the configured public-directory prefix. An unauthenticated requester can therefore retrieve a sibling prerendered HTML page when that page contains the Angular SSG marker. The issue is limited to Windows deployments that pass relative request URLs to CommonEngine.render, have a prefix-sharing sibling output directory, and contain qualifying prerendered Angular HTML; it does not provide arbitrary file read. This issue is fixed in versions 20.3.36, 21.2.23, and 22.1.7.	N/A	More Details
CVE-2026-95137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2026-101322	In Eclipse BaSyx AAS Web UI versions v2-241220 through releases before v2-260924, the shared request handler attached the selected infrastructure's `Authorization` header to outgoing requests without checking the destination origin. In deployments using authentication, an attacker could induce a user to open a crafted Web UI link whose `aas` or `path` query parameter points to an attacker-controlled endpoint. The user's browser would then send the configured Basic Authentication credentials, Bearer token, or an available OAuth2 access token to that endpoint. The attacker could reuse the disclosed credential to access protected AAS services with the victim's privileges. The issue is fixed in v2-260924.	N/A	More Details
CVE-2026-18734	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-2026-94620	Classroom 50 is a free and open-source tool for managing and grading programming assignments via GitHub. Prior to version 1.11.0, `gh teacher download` clones each student's assignment repository and then writes autograde artifacts (`result.json` and `results.json`) into the just-cloned working tree. The write followed symlinks, so a student who committed `result.json` or `results.json` as a **symlink** (materialized verbatim by `git clone`) could redirect the teacher's write to an arbitrary path — e.g. `~/zshrc`, `~/ssh/authorized_keys`, a cron file, or an in-clone `.git/hooks/*` file that git subsequently executes. The written bytes are attacker-controlled (the student's uploaded release asset for `result.json`; student-chosen submit-tag names for `results.json`). This is an arbitrary file write leading to code execution as the teacher, whose `gh` token carries `admin:org`, `repo`, and `workflow` across the entire classroom organization. Version 1.11.0 contains a patch. Some workarounds are available. Avoid running `gh teacher download` against untrusted student repositories, or run it inside a disposable sandbox / container with no access to sensitive host files or credentials. Inspect cloned trees for symlinked, hardlinked, or special (`result.json`/`results.json`) entries before allowing the artifact-refresh step to run.	N/A	More Details
CVE-2026-64818	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-104859	Nx is a monorepo solution for TypeScript and polyglot codebases. From 21.4.0 until 22.7.8 and from 23.0.0 until 23.1.1, the @nx/docker release pipeline builds docker tag, image lookup, and docker push invocations as shell command strings. The release.docker.repositoryName and registryUrl configuration values are interpolated into those strings and passed to /bin/sh -c, allowing shell syntax in untrusted Nx configuration to execute during nx release version or nx release publish. A pull request or repository configuration change can therefore execute commands with the release job's privileges and expose registry credentials or cloud tokens, and dry-run publishing does not prevent the vulnerable pre-check command from executing. This issue is fixed in versions 22.7.8 and 23.1.1.	N/A	More Details
CVE-2026-104855	Wasmtime is a runtime for WebAssembly. From 46.0.0 until 46.0.2 and 47.0.3, fuel and epoch preemption checks inside bulk operations including memory.copy, table.grow, and array.copy can expose invalid intermediate state when an embedder mutates a Store in Store::epoch_deadline_callback or continues using a Store after cancellation or a trap. A cancelled non-nullable table growth can leave null elements, linear-memory growth during memory.copy can invalidate retained raw pointers, and callback-triggered garbage collection during array.copy can invalidate GC pointers, resulting in a crash, invalid memory access, or GC heap corruption. Embeddings whose callbacks only access the host data in Store<T>, and embeddings that discard a Store after timeout or epoch deadline, are not affected. This issue is fixed in versions 46.0.2 and 47.0.3.	N/A	More Details
CVE-			

2026-27874	: Use of Hard-coded Credentials vulnerability in Johnson Controls EasyIO FS32 allows : Exploitation of Default or Hard-coded Credentials. This issue affects EasyIO FS32: before 3.0b63.	N/A	More Details
------------	--	-----	------------------------------